

**ITU Regional Forum on Consumer Information,
Protection and Rights for Africa 2017
Cotonou, BENIN
14-16 March 2017**

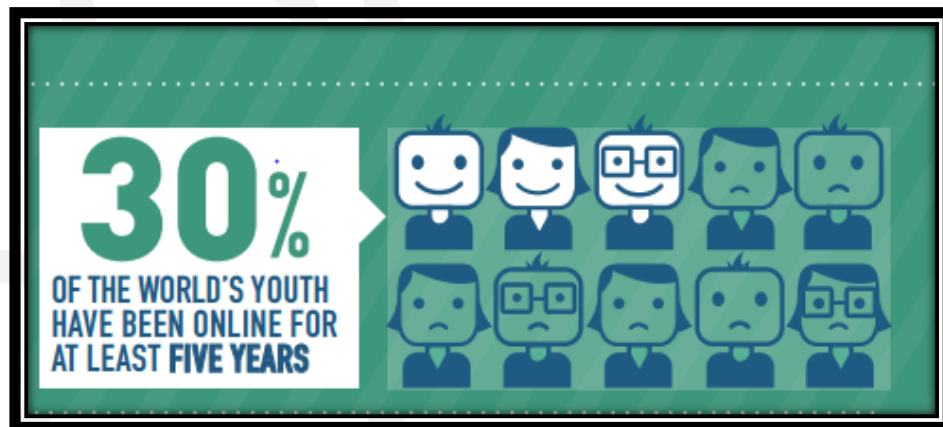
**The need of an international framework for
cooperation: the Child Online Protection (COP)
Initiative & Guidelines**

Anne Rita SSEMBOGA
ITU REGIONAL OFFICE FOR AFRICA
anne,rita.ssemboga@itu.int



Why COP

- Children are going online more than ever.
- Technology is readily available to children at a young age
- Being at ease with technology, children can easily bypass restrictions.
- Cybercrime is borderless, invisible and organized



Today, the use of Information and Communication Technologies (ICTs) is the key to access **information society**



**Real-time
Information**

Libraries

**On-line public
services**

**Personal
communication**

Entertainment

Media

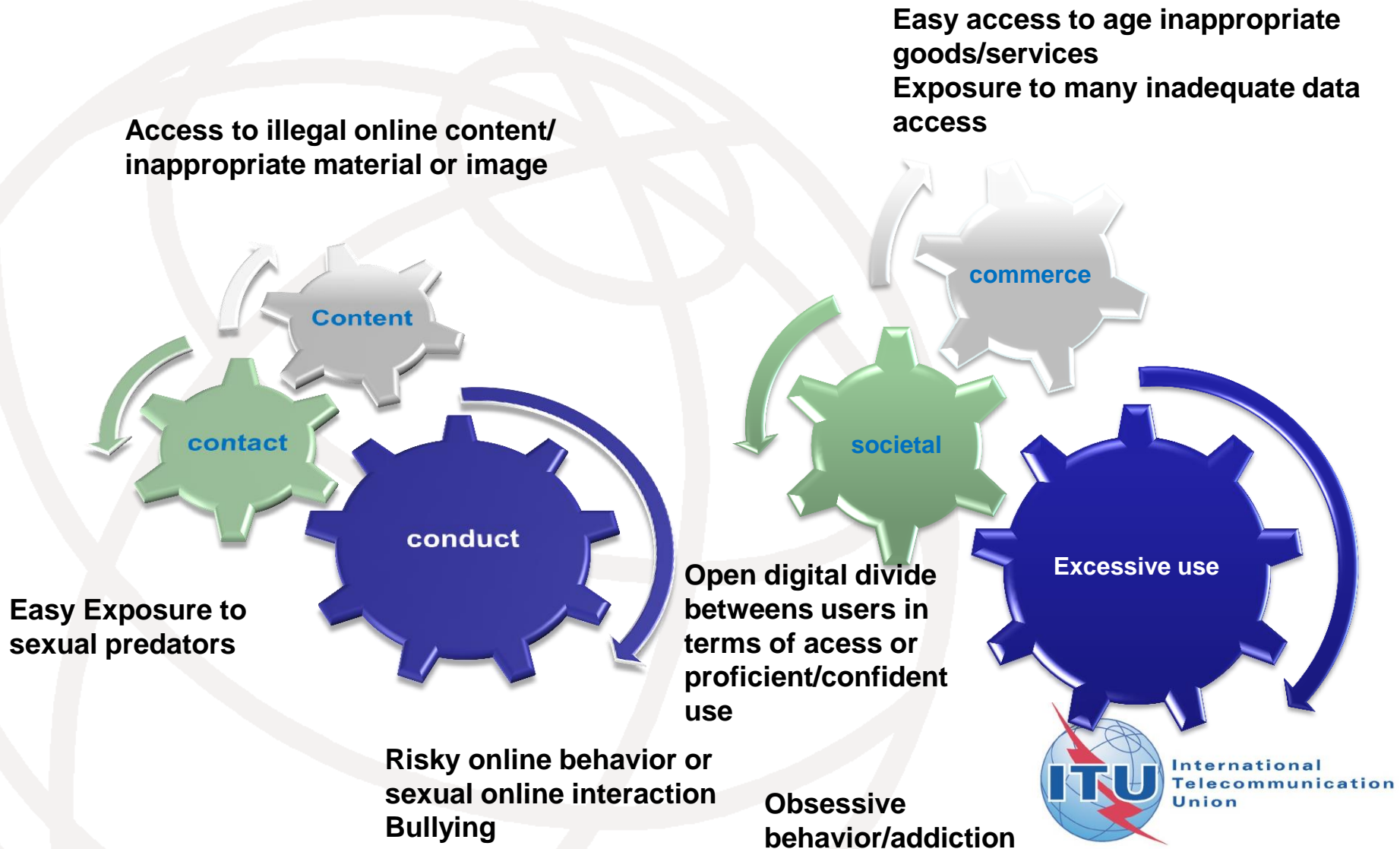
Databases

**Social and
professional
networks**

Social media



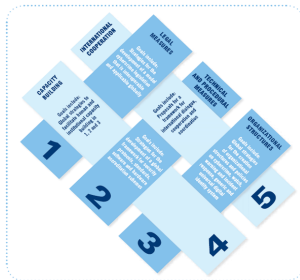
Key risks to children online



ITU's mandate on Cybersecurity

2003 – 2005

WSIS entrusted ITU as sole facilitator for WSIS Action Line C5 -
“**Building Confidence and Security in the use of ICTs**”



2007

Global Cybersecurity Agenda (GCA) was launched by ITU Secretary General
The GCA is a **framework for international cooperation in cybersecurity**

The COP initiative is part of the Global cybersecurity agenda(GCA)

Building confidence and security in the use of ICTs is widely present in **ITU** resolutions. In particular several **ITU Conferences (ITU Plenipotentiary- PP, WTSA, and WTDC)** have produced Resolutions (PP Res 130, 174, 179, 181, WTSA Res 50, 52, 58, and WTDC 45, 67, 69) touching on the most relevant ICT security related issues, from legal to policy, to technical and organization measures.

The Child Online Protection (COP) Initiative

The **COP Initiative** aims at bringing together partners from all sectors of the global community to ensure a safe and secure online experience for children everywhere.

Objectives

- **Identify risks and vulnerabilities to children in cyberspace;**
 - **Create awareness of the risks and issues through multiple channels;**
 - **Develop practical tools to help governments, organizations and educators minimize risk; and**
 - **Share knowledge and experience while facilitating international strategic partnership to define and implement concrete initiatives**
-

Coordinated Response

Need for a multi-level response to the cybersecurity challenges



We count on the support of several partners...



vodafone

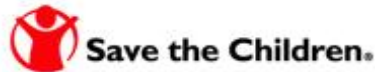


Microsoft

Telefonica



ins@fe



Council Working Group (CWG) on COP

- ❑ The CWG COP is a **platform which facilitates the membership's input and guidance on ITU's role in child online protection**. Through the work of the Group, our membership makes recommendations and provide invaluable inputs to the Initiative.
- ❑ The last **Plenipotentiary Conference**, held in Busan in 2014, made some important amendments:
 - participation in the Group meetings will be open to all stakeholders (both ITU members and non-members);
 - all documentation will be publicly available without password protection

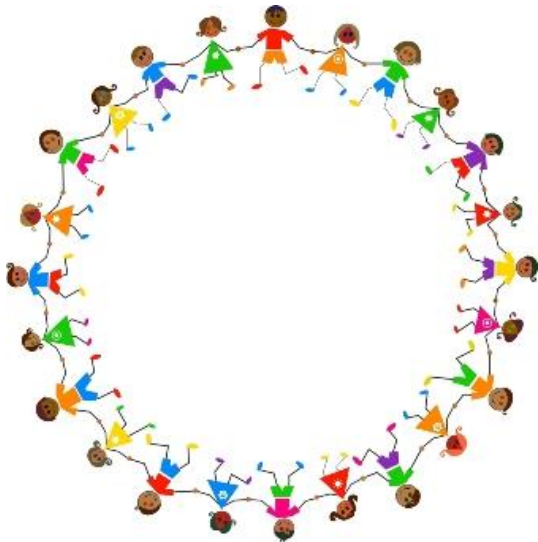


Next CWG-COP Meeting

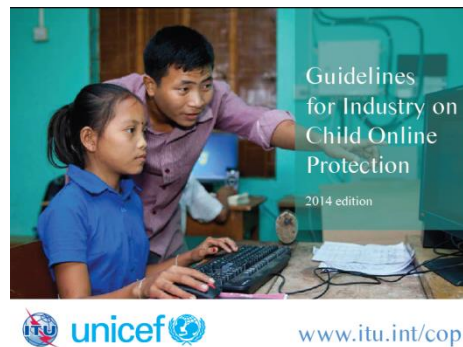
30 September 2015



What do we do?



4 Set of COP Guidelines



- Developed in cooperation with COP partners, is the first set of guidelines addressing different stakeholders. [Available in the six UN languages](#)

The COP Guidelines in details

COP Guidelines for Children



Children and young people need to be aware of risks online. The guidelines advise them on possible harmful activities online, such as bullying and harassment, identity theft, and online abuse. The guidelines also include advice to children seeing and experiencing harmful and illegal content online, or young people being exposed to grooming for sexual purposes, the production, distribution and collection of child abuse material.

The COP Guidelines in details

COP Guidelines for Parents, Guardians and Educators



Guidelines for
Parents, Guardians
and Educators on
Child Online
Protection



www.itu.int/cop

Research shows that more and more children are connecting to the Internet using game consoles and mobile devices, yet many adults are not even aware that these activities include internet connectivity. The guidelines for parents, guardians and educators provide recommendations on what they can do to make their child's online experience a positive one.

The COP Guidelines in details

COP Guidelines for Policy Makers



The guidelines for policy makers will help individual countries plan for their strategies for child online protection in the short, medium and longer term. In order to formulate a national strategy focusing on online child safety, policy makers need to consider a range of strategies, including establishing a legal framework; developing law enforcement capabilities; putting in place appropriate resources and reporting mechanisms; and providing education and awareness resources.

The COP Guidelines in details

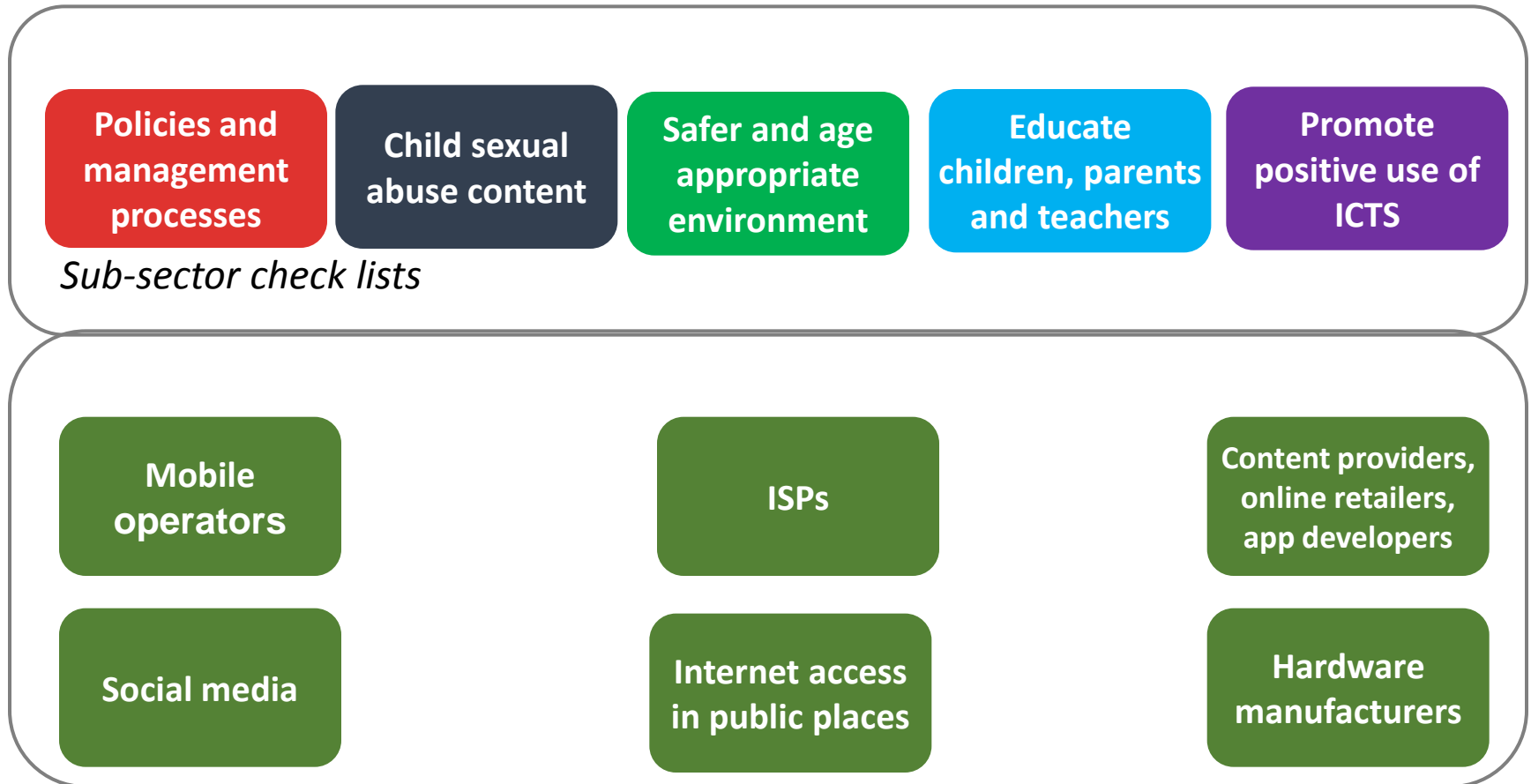
New COP Guidelines for Industry



The updated guidelines for Industry on Child Online Protection provide advice on how the ICT industry can help promote safety for children using the Internet or any technologies or devices that can connect to it. **An online platform of COP case studies from the broader ICT Industry further complements the content of these Guidelines.**

ITU & UNICEF new version of the Guidelines for Industry

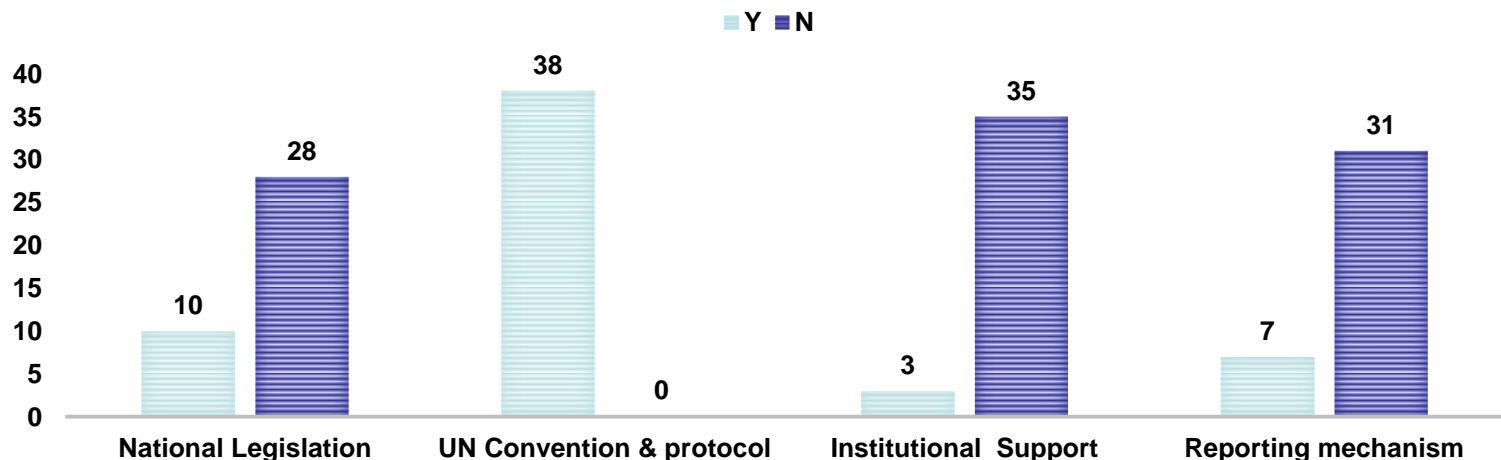
How are the Guidelines structured?



Child online country profile wellness

- Cybersecurity wellness profile provide an overview of the country level cybersecurity development based on the 5 pillars of the GCA and the Information on Child online protection initiative is also covered.
- Currently 195 country profiles are available based on GCI 2014 data and the graph below is the COP wellness profile for Africa (38 countries)

COP country wellness profile for Africa



Assisting countries to establish national strategies and policies

- Cameroon
- Ghana
- Mauritius
- Sierra Leone
- Gambia
- Oman
- Brunei
- Zambia
- Bahrain
- Chad
- Gabon
- Rwanda



Key stakeholders to ensure children online safety at national level



Specificities/ characteristic of each stakeholders (1)

Children

- Comfortable with Internet & Technology devices
- inexperienced

There is a need to develop policy at a national level to protect and ensure children safe use of Internet

Parents/guardians

Little lost when it comes to technology/Internet use

Need to be informed about risks and advantages of new technologies & Internet through different communication channels

Educators

Responsibility to teach children about how to stay safer online at home/school or anywhere else

Need professional training linked to 1st class, up to date teaching resources

Specificities/ characteristic of each stakeholders (2)

Industry

Have expertise and knowledge of their products/services

- Should promote awareness of the online & safety issues to community
- Should identify hazards in their products and services and correct them

Research community

Have the knowledge of technical and social aspects and impact of the Internet

- Can help national government and policy makers develop strategies based on hard facts & evidence
- Can be an intellectual counterweight to the industry

NGO

Have the Expertise and information which can be an invaluable resources in reaching out & providing services to the community

Can help promote the online safety agenda

Specificities/characteristic of each stakeholders(3)

Law Enforcement

Should be fully engaged with any overall strategy to help make the internet safer

- Need to be trained appropriately to conduct investigations into internet related crimes against children and youth
- Need the right level of technical knowledge and access to forensic facilities to extract and interpret data obtained from technologies devices
- Should establish clear reporting mechanism (hotline)

Social services

Can provide support and counselling to abused or harmed children/youth online

Professional working with the social services need appropriate training to be able to provide this kind of support

National Checklist

Comprehensive legal framework

- Laws should make it clear that any and every crime that can be committed in the real world can also be committed online
- Developed new laws or adapt existing ones to outlaw internet specific offense such as grooming, perform or watch sexual acts
- Outlaws the misuse of computers for criminal ends

Need for a national focus on online child protection

- Bring together all of the key stakeholders and players to develop and implement a national initiative/strategy for children online safety
- Establish a self or co-regulatory model by publishing codes or good practices to guide Internet industry on measures to be taken to keep children safer online
- Involve the mass media in promoting awareness messages and campaigns

Need to develop local resources

- To reflect national laws and local cultural norms to take into consideration language and cultural barriers
- Essential for any Internet safety campaign or training material developed

Need for public education and awareness activities

- Educational & outreach programs should be developed for professional, parents/guardians/educators to help build awareness on the issues and provide strategy to deal with them
- Ensure safety material are made available in either in written forms or produce using other media such as video
- Important to strike the right tone for any education and awareness campaign

Need for reporting mechanisms for online predatory behavior including bullying

- Mechanism for reporting abuse of an online services or illegal online behavior should be widely promoted online and using other medias.
- Possibility for people who feel threaten in any way or who have witness any worrying activity on the Internet to report quickly to the relevant law enforcement agencies(who should be trained and ready to respond.

Helping children to stay safe online through the use of technical tools

- Numbers of free software programs can help screen out unwanted materials or block unwanted contact .as they as generally part of the operating system or provided as part of a package from ISP.
- Technical tools should be use as part of a global arsenal as parent/guardian involvement is critical.

MOBILE OPERATORS



Mobile operators enable access to the Internet as well as offer a range of mobile-specific data services. Many operators have already signed up to COP codes of practice, and offer a range of tools and information resources to support their commitments.

[See relevant case studies >](#)

INTERNET SERVICE PROVIDERS



Internet service providers act as both a conduit, providing access to and from the Internet, and a repository for data through their hosting, caching and storage services. As a result, they have been in the forefront of accepting responsibility for protecting children online.

[See relevant case studies >](#)

CONTENT PROVIDERS, ONLINE RETAILERS AND APPLICATIONS (APP) DEVELOPERS



The Internet provides all types of content and activities, many of which are intended for children. Content providers, online retailers and app developers have tremendous opportunities to build safety and privacy into their offerings for children and young people.

[See relevant case studies >](#)

USER-GENERATED CONTENT, INTERACTIVE AND SOCIAL MEDIA SERVICE PROVIDERS



Children and adolescents are major participants, on multiple platforms, in creating and sharing content. User-generated content, interactive and social media service providers can set policies and take actions to enhance child online protection and participation.

[See relevant case studies >](#)

NATIONAL AND PUBLIC SERVICE BROADCASTERS



Children and young people are a significant audience for content developed by broadcasting services, which is increasingly accessible online. National and public service broadcasters are working to offer the same level of security for online viewing that is applied to television and radio.

[See relevant case studies >](#)

HARDWARE MANUFACTURERS, OPERATING SYSTEM DEVELOPERS, AND APP STORES



Children today are accessing the Internet through an array of electronic devices. Hardware manufacturers, OS Developers and App Stores can provide built-in technical mechanisms along with educational and empowerment activities in order to promote a safer online environment for children.

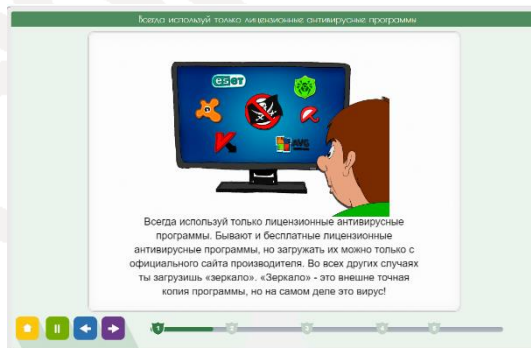
[See relevant case studies >](#)

Online Platform of Case Studies

Regional activities



Regional annual Capacity-building Workshop on Child Online Safety(COS) for Africa Sub-Saharan countries
Lilongwe, Malawi, 18-20 July 2016



In 2015, ITU-D Sector Member ONAT launched an online and offline course titled “Multimedia distance-learning course on the safe use of Internet resources”



**CYBERSECURITY
IN ROMANIA**
- CONGRESS -
SIBIU, 13-16 SEPTEMBER 2016

Cybersecurity in Romania- Congress in Sibiu
(September 2016)



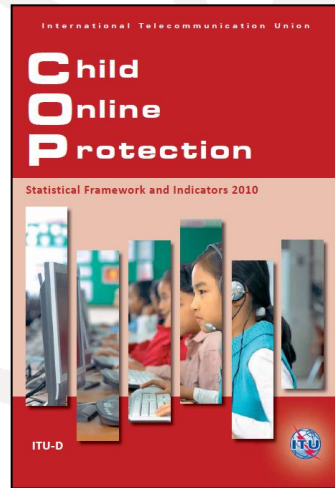
Other projects



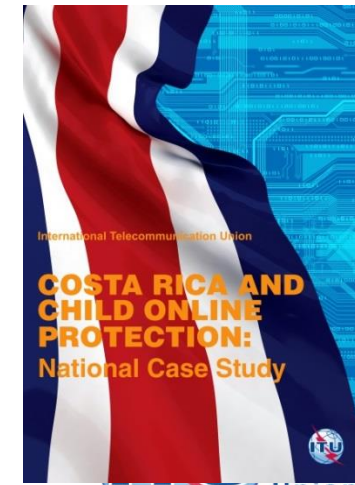
Share a platform of countries profiles



Run surveys with policy makers



Data collection



Develop case studies

For more information please visit:
www.itu.int/COP

Thank you

