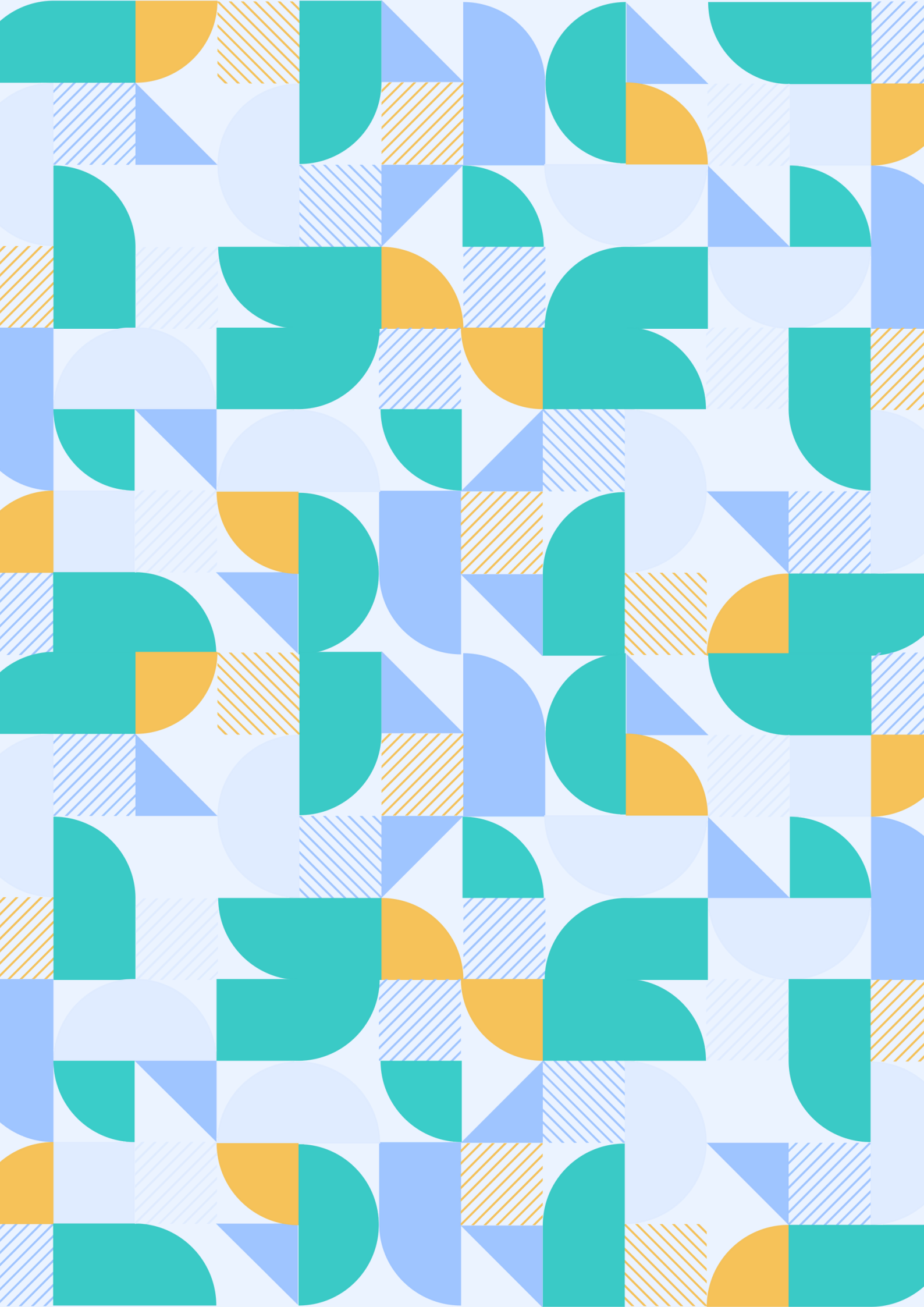


Child Online Safeguarding Policy Guidebook

Toolkit for ISPs





Child Online Safeguarding Policy Guidebook

Toolkit for ISPs

The Editorial Team

Joie Cruz
Project Lead

Uriel Sunga
Editorial Lead

Katrina Ang
Design Lead

Francesca Lee
Illustrator

Toolkit designed by Limitess Lab





Table of Contents

02

**Definition of
Terms**

10

**The Problem in
COSP in the
Philippines**

11

**Child Online
Safety Statistics
by the Philippine
Kids Survey 2021**

12

**COSP's Salient
Features in a
Glance**

13

**Unacceptable
Uses of the Free
WiFi**

14

**The Role of ISPs
in COSP**

16

**10 Types of
Cyberbullying**

17

**About the
Internet Watch
Foundation**

19

Contact Details

Definition of Terms



For the purposes of this Toolkit, the following terms are defined, to wit.

"Whitelist"

"Whitelist" refers to the DICT-curated list of software, domains, or network addresses which are deemed safe to access via the Free Internet Access in Public Places (FIAPP) Program for public educational institutions. For public educational institutions, access under the FIAPP Program to items outside the Allow List shall be restricted, in accordance with the provisions of this Circular and other relevant issuances.

"Blacklist"

"Blacklist" refers to the DICT-curated list of software, domains, or network addresses which are prohibited or restricted from being accessed via the FIAPP Program. Any item outside of the Blacklist may be accessed through the FIAPP Program.

"Authority" or "Authorities"

"Authority" or "Authorities" refers to the government agency or agencies in charge of law implementation and enforcement, including but not limited to the Department of Information and Communications Technology (DICT), Department of Justice (DOJ), Department of Social Welfare and Development (DSWD), Department of Education (DepEd), Philippine National Police (PNP), National Bureau of Investigation (NBI), Local Government Units (LGUs), among 'other government instrumentalities, in accordance with their respective jurisdictions. In a limited sense, the term shall also refer to the technical personnel in charge or on duty, who are tasked with providing the information service network for the free public Internet under the FIAPP Program.



The government authorities in charge of Child Online Safeguarding (COSP) and the Free Internet Access in Public Places (FIAPP) Program.

Source: DICT Department Circular No. 015

“Captive Portal”

“Captive Portal” refers to the initial web page displayed to end-users who connect to a public Internet access point, to which the end-user is obliged to view and interact with before being granted broader access to the Internet. The term likewise refers to a “Splash page,” “Log-In page,” “Splash portal,” or “Landing page.”



Examples of captive portals produced by the Department of Information and Technology (DICT).

“CHED”

“CHED” refers to the Commission on Higher Education, which handles educational institutions and the implementation of COSP in said establishments.



“Child” or “Children”

“Child” or “Children” refers to a person below eighteen (18) years of age. The term shall likewise include persons who are eighteen (18) years of age or older but are unable to fully take care of themselves from abuse, neglect, cruelty, exploitation, or discrimination due to physical or mental disability or condition.

“Child-inappropriate content”

“Child-inappropriate content” refers to any material which: (a) is illegal, or (b) though not illegal, may nevertheless be harmful or detrimental to, or may otherwise endanger, the well-being of children. The term includes, but is not limited to, content that:

- exposes children to scams, identity theft, pornography, explicit content, hate speech, harassment, discrimination, cybercrimes, or other similar activities;
- encourages children to do unnecessary harm or violence upon themselves or to other persons; or
- enables children to acquire goods or services, or to enter into any other transaction, which they would not otherwise be able to do in person and without the consent of their parents or the persons exercising parental authority over them.

“Child Pornography”

“Child Pornography” refers to any representation, whether visual, audio, written, or a combination thereof, by electronic, mechanical, digital, optical, magnetic, or any other means, of a child, engaged or involved in real or simulated explicit sexual activities," as defined under RA 9775 and other applicable laws, circulars, rules, and regulations. Consistent with RA 9775 and other existing laws, the term shall include any pornographic material wherein:

- a person, regardless of age, is presented, depicted, or portrayed as a child; or
- a computer-generated, digitally or manually crafted, image or graphics of a person is represented or made to appear as a child.

“Child sexual exploitation material”

“Child sexual exploitation material” or “CSEM” refers to materials depicting child sexual abuse, sexualized content depicting children, and other similar lewd materials.

"CICC"

“CICC” refers to the Cybercrime Investigation and Coordinating Center, an agency attached to the DICT which is in charge of monitoring cybercrime cases banded by law enforcement and prosecution agencies.



"COSP”

“COSP” refers to the Child Online Safeguarding Policy for the FIAPP Act, instituted under this Department Circular and such other related departmental issuances that may be issued in connection therewith.

"CSOs”

“CSOs” refer to Civil Society Organizations who may be part of COSP’s external stakeholders.

"Data Privacy Laws”

“Data Privacy Laws” refers to RA 10173, otherwise known as the “Data Privacy Act of 2012,” its amendments, and other applicable statutes, circulars, rules and regulations for the protection of data privacy and security.

"DepEd”

“DepEd” refers to the Department of Education who handles Philippines’ primary and secondary educational system and how COSP is to be implemented as the country’s educational resource.



“DICT”

“DICT” refers to the Department of Information and Communications Technology as the sector that implemented COSP.



"DOJ”

“DOJ” refers to the Department of Justice who are responsible for upholding the rule of law in the country.



"DSWD”

“DSWD” refers to the Department of Social Welfare and Development who are responsible for the welfare of children in the country.



"FIAPP Act”

“FIAPP Act” refers to RA 10929, otherwise known as the “Free Internet Access in Public Places Act.”

"FIAPP Program"

“FIAPP Program” refers to the Free Internet Access in Public Places Program under RA 10929 or the FIAPP Act which grants Free Wifi in selected public areas in the Philippines.



Official logo of the FIAPP Act

“Free public Internet access points”

“Free public Internet access points” refers to the public places where the Free Internet under the FIAPP Program is deployed.

“IACACP”

“IACACP” refers to the Inter-Agency Council Against Child Pornography which is in charge of coordinating, monitoring, and overseeing the implementation of RA 9775 or the Anti-Child Pornography Act of 2009.



“IRR”

“IRR” refers to Implementing Rules and Regulations which in this case, facilitates the implementation of R.A. 10929 or the Free Internet Access in Public Places Act.

“ISPs”

“ISPs” refer to Internet Service Providers as defined under existing laws, circulars, rules, and regulations; examples which consist of Globe, PLDT, Converge, etc.

“LGU”

“LGU” refers to the Local Government Unit which represents a certain community which may be a barangay, a town or city, or a municipality.

“NBI”

“NBI” refers to the National Bureau of Investigation which is in charge of investigating major criminal cases in the Philippines.



“NGAs”

“NGAs” refers to National Government Agencies which are units of the National Government.

“NGOs”

“NGOs” refer to Non-Governmental Organizations who may be part of COSP’s external stakeholders.

“NPC”

“NPC” refers to the National Privacy Commission, an agency attached to the DICT in charge of monitoring data protection.



“NTC”

“NTC” refers to the National Telecommunications Commission, an agency attached to the DICT in charge of monitoring telecommunications, television, and radio networks in the country.



“Online Child Safety Zones”

“Online Child Safety Zones” are websites or applications that are designed for the use of children with built-in features that promote and ensure the privacy and safety of the end-user child.

“Online Risks to Children”

“Online Risks to Children” are classified into four (4) categories of risks, namely: Content, Contact, Conduct, and Contract:

1. **Content Risk** exists when a child is exposed to child-inappropriate content, such as lewd or explicit images;
2. **Contact Risk** exists when a child participates in communication that puts him or her at risk, such as with cyber predators or persons soliciting a child for exploitative purposes;
3. **Conduct Risk** exists when a child behaves or tends to behave in a way that directly contributes towards Content or Contact Risk;
4. **Contract Risk** exists when a child is deliberately victimized by other online entities.

“Parent”

“Parent” refers generally to the mother or father of the child. The term shall likewise include the legal guardian, grandparent, or any other person exercising parental authority or responsibility over the child.



“Person”

“Person” refers to any individual, partnership, corporation, trust, estate, cooperative, association, or other entity, whether natural or juridical.

“Peer-to-Peer Exchange”

“Peer-to-Peer Exchange” refers to an exchange of information or content using a peer-to-peer network.

“Peer-to-Peer Network” or “P2P”

“Peer-to-Peer Network” or “P2P” exists when two (2) or more computer systems are connected to each other, essentially sharing their resources, thereby enabling the transfer of data or information from one system to the other or others, and vice-versa, without going through a separate server.

“Personal Information”

“Personal Information” refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information or when put together with other information would directly and certainly identify an individual.

“PNP”

“PNP” refers to the Philippine National Police, the armed police in the country.

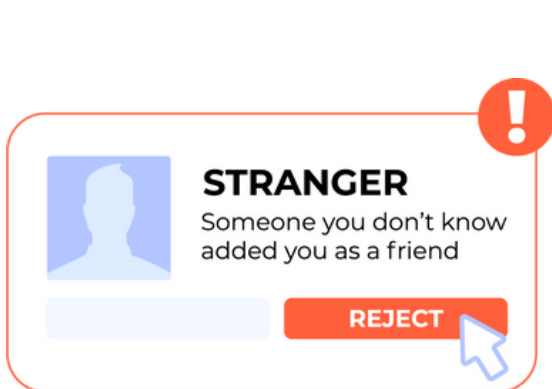


“PNP-ACG”

“PNP-ACG” refers to the PNP Anti-Cybercrime Group, the agency in charge of Cyber response and security, as well as digital forensics.

“Responsible Digital Citizenship”

“Responsible Digital Citizenship” means possession of online social skills to take part in the online community life in an ethical and respectful way, inclusive of behaving lawfully, protecting one’s privacy and those of others, recognizing one’s rights and responsibilities in the use of digital media, and mindfulness of how one’s online behavior and activities affect one’s self, others, and the wider online community.



“Safeguarding”

“Safeguarding” refers to putting and further developing precautionary systems, mechanisms, stipulations, devices, technologies, or other similar protective measures in place in order to prevent or mitigate unwanted or harmful incidents against children as well as address concerns regarding these circumstances.

“SUCs”

“SUCs” refers to State Universities and Colleges which are institutions for higher education.

“TESDA”

“TESDA” refers to the Technical Education and Skills Development Authority in charge of supervising and managing the country’s Technical Education and Skills Development.



“Terms of Use”

“Terms of Use” refers to the legal agreements between a service provider and a person who wants to use that service. The person must agree to abide by the Terms of Use in order to use the offered service. The term likewise refers to “Terms of Service,” “Terms and Conditions,” commonly abbreviated as ToU, ToS, or T&C.

“Virtual Private Network (VPN)”

“Virtual Private Network (VPN)” refers to a service that creates an encrypted connection that extends a private network across a public network, thereby enabling its users to preserve their anonymity online, circumvent geographic-based and other restrictions on the public network, as well as send and receive data across shared or public networks as if their devices were directly connected to the private network.



The Problem of COSP in the Philippines

How safe are Filipino children online?

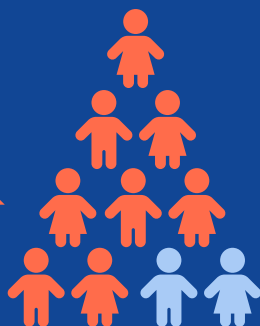
TOP 1
IN THE WORLD

Rank held by the Philippines as the source of Child Sexual Abuse Material



LESS THAN 1 IN 2

feel safe using the internet



8/10

FILIPINO CHILDREN & TEENAGERS

are in danger of cyberbullying or online sexual abuse



25%

OF FILIPINO CHILDREN

have encountered sexual images online last 2020

What is being done?

RA 7610

The Special Protection of Children Against Abuse, Exploitation and Discrimination Act

RA 7610 and the Child Online Safeguarding Policy has provisions for protection of children from abuse, exploitation, and discrimination.

Child Online SAFEGUARDING

The DICT has enacted COSP which aims to protect all Filipinos, especially children, from child-inappropriate materials accessible on the Free Internet, and soon, on the Philippines' internet!

Source: Philippine Kids Online Survey 2021, hosted by UNICEF

Child Online Safety Statistics by the Philippine Kids Survey 2021

Source: Philippine Kids Online Survey 2021, hosted by UNICEF



10 YEARS OLD

Average age that Filipino kids start going online



2 HOURS PER DAY

Average time Filipino children spend on the internet

What do Filipino kids use the internet for?



Schoolwork



Social Media



Children in Social Media vs Gaming



6/10 CHILDREN ON SOCIAL MEDIA

Connect with people they meet online

8/10 CHILDREN PLAYING ONLINE GAMES

connect with people they meet online

1/10 CHILDREN ON SOCIAL MEDIA

Accept friend requests from strangers

4/10 CHILDREN PLAY GAMES

without supervision

What do children see and experience online?



MORE THAN 5

Landed on websites not knowing how they got there



1/7 CHILDREN

Received sexual messages last 2020



1/4 CHILDREN

Encountered sexual images online



1/5 CHILDREN

Experienced something upsetting online

COSP's Salient Features at a Glance

Child Online Safeguarding for the FIAPP

COSP PROTECTS CHILDREN'S RIGHTS THROUGH THE

PREVENTION

REDUCTION

BLOCKING

of harmful websites which promote child abuse, cruelty, and exploitation that may be accessed through the Free Internet Access in Public Places Program

Scope of COSP Implementation

COSP is implemented by the following internal stakeholders:



National Government Agencies



Local Government Units



Civil Service Organizations



Non-Government Organizations



State Universities and Colleges



Internet Service Providers in the FIAPP program

The provisions of COSP also extend to everywhere that FIAPP is implemented.

FIAPP as a Service



Free Public Internet Safety and Protection

Free Public WiFi will be available on all selected FIAPP institutions and are subject to all laws and guiding principles of COSP under the FIAPP.



COSP Website

A child-friendly website dedicated to Child Online Protection that aims to inform and educate Parents, Children, NGOs, and ISPs while also protecting children and teens online through reporting mechanisms and hotlines.



COSP Captive Portal

A COSP-exclusive captive portal will be developed in order to further protect children from online harm. Anyone who connects to the captive portal will be required to follow its terms and conditions.

Unacceptable Uses of the Free WiFi

COSP aims to protect children from the following:

Illegal Usage



Hacking

Attempting to access a user's profile without their consent



Phishing

Sending malicious links with intent to steal information.



Identity Theft

Using stolen information to pose as someone



Threats

A form of cyberbullying which threatens the victim with physical violence.



Spamming

Attempting to access a user's profile without their consent



Harassment

Aggressive and constant intimidation and pressure.



Copyright Infringement

Usage of copyrighted works without permission.



Gambling

Wagering on events with uncertain outcomes with the intent of winning something of value.



Discrimination

A form of cyberbullying which excludes the victim due to their appearance, race, gender, situation and more.



Blackmail

A form of cyberbullying which threatens the victim with the release of sensitive material or information.



Other unlawful use

All other manners of usage contrary to existing laws.

Harmful Content



Pornography

Videos or Images showing sexual acts in a non-educational manner.



Child Sexual Abuse Material

Videos or Images showing sexual, physical, or other forms of child abuse



Fake News

News articles which aim to spread false information or propaganda.

What are your Roles and Responsibilities?

The Philippines' Internet has had a lack of security measures to protect its citizens for a while now and there have been steps to address this to ensure the growth of the Filipino people and empower them through the Free Internet for All program.

Several major Philippine ISPs have pledged their support for the Free Internet for All program and the Child Online Safeguarding Policy, but aside from providing the Free Internet access, what can ISPs do to protect children and teens online?

ISPs have several responsibilities, like gatekeeping content, marking child-inappropriate content, on top of ensuring that their service is effective, but more than this, they are also expected to try to make their implementation as efficient as possible.

ISP Checklist



Compliance with RA 9775 or the “Anti-Child Pornography Act of 2009”

Comply with all international treaties to which the Philippines is a signatory or a State party concerning children’s rights including:

- Convention on the Rights of the Child
- Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography
- International Labor Organization (ILO) Convention No. 182 on the Elimination of the Worst Forms of Child Labor
- Convention Against Transnational Organized Crime.

ADDITIONAL INFORMATION

You can read and access the **RA 9775** through the following link:

www.officialgazette.gov.ph/2009/11/17/republic-act-no-9775-s-2009/



Control child-inappropriate content online

Ensure that inappropriate content such as sexually explicit material, is regulated and marked as so online in a clear manner to prevent accidental access.



Employ processes for child online safety

Carry out mechanisms, procedures, and tools such as parental controls and age verification to ensure the safety and freedom of children online such as age verification and parental consent.



Promote and utilize safe websites

As far as practicable, utilize only websites that ensure and promote safe participation and self-expression to foster a wholesome and educational online environment for children and teenagers.



Comply with COSP and other issuances relating to FIAPP

Follow the provisions of all existing and future laws, circulars, orders, rules, and regulations relating to the safeguarding of children online.

ADDITIONAL INFORMATION

To know more about COSP, you may visit these links:

DICT Circular No. 15 - www.bit.ly/COSP-DICT-Circular


COSP Presentation - www.bit.ly/COSP-Presentation

COSP Primer - www.bit.ly/COSP-Primer

To know more about child online abuse and exploitation, you may visit this link:

Sonia Livingstone Framework of Child Online Abuse and Exploitation - www.bit.ly/coae-framework





10 Types of Cyberbullying



Exclusion

The act of leaving someone out deliberately.

Example: Exclusion of a person in an online group while others mutually are invited



Harassment

Aggressive and constant intimidation and pressure.

Example: Constant hurtful and threatening comments on every post of one person



Outing / Doxing

The act of publicly revealing a person's sensitive or personal information.

Example: Spreading sensitive and personal info of someone on a public post without their consent.



Trickery

The act of befriending or lulling a target with a false sense of security then betraying their trust.

Example: Publicly sharing of photos privately shared to you by someone online



Cyberstalking

The act of using the internet to monitor, watch and harass everything about another person.

Example: Following the target online by joining the same groups and forums and harassing someone under different accounts.



Frapping

Using someone's social media account/s to post inappropriate content.

Example: Posting offensive and hurtful slurs to ruin the reputation of the real owner of said social media account.



Masquerading

Using a fake account or identity for the purpose of bullying someone and hiding their identity.

Example: Using a fake account to post offensive comments on someone's profile



Dissing

Posting or spreading cruel information about someone publicly or privately online to ruin their relationships or reputation.

Example: Publicly shaming someone online for being a certain race



Trolling

The act of intentionally upsetting others or strangers through offensive comments.

Example: Posting offensive comments on several articles to insight anger on users.



Flaming

Posting or chatting insults or profanity directly to the victim.

Example: Someone flames a person online for being new or inexperienced in a game.

Source: www.blog.securly.com/2018/10/04/the-10-types-of-cyberbullying/

About the Internet Watch Foundation



What is the Internet Watch Foundation (IWF)?

Source: www.iwf.org.uk

IWF is a charity who works:



to stop the repeated victimisation of people abused in childhood



to make the internet a safer place

by identifying & removing global online child sexual abuse imagery.



170+

MEMBERS OF IWF

Among which are international giants from the internet industry such as Google, Apple, Amazon, and more.

IWF at a Glance

50

GLOBAL EXPERTS IN IWF

working to keep the internet safe

25

YEARS & COUNTING

since IWF was first founded in 1996

OVER

6000

REPORTS PER WEEK

are being assessed by the IWF team

Notable Members of IWF



Globe



CONVERGE



CISCO

amazon.com

DNSFilter



PLDT



Smart



Meta



Microsoft



How does IWF remove content?

1 Assessing Content



Reported sites and content are analyzed, every 2 minutes, by experts and enforcing bodies around the globe

2 Tracing, locating, and removing content



Use technical internet tracing to determine the location of the host server of the reported content.



Details are delivered to relevant authorities or acted upon via partnership with the company whose services are abused.

Why join IWF?



IWF has reduced UK's child sexual abuse imagery to

0.1%

**FROM 18% OF
WORLD'S TOTAL**

IWF HAS ALSO RECEIVED FUNDING FROM:



European Union



Childnet
International

AMONG OTHERS

Membership Benefits

Source: www.iwf.org.uk/membership/benefits-of-membership/

1

Reduce the risk of users finding illegal imagery online.

2

Usage of IWF tools to help you fight criminal images and videos online.

3

On-call IWF expert for all your inquiries.

4

Keep your websites free from child sexual abuse imagery.

5

Access to IWF research, intelligence, and data.

6

Recognition as one of the 170+ global tech partners of IWF.

Contact Details

Department of Information and Communications Technology

- 📞 **Information Division:** 8-920-0101 local 1004
- 📞 **Trunkline:** 8-920-0101
- ✉️ information@dict.gov.ph
- 👉 www.dict.gov.ph/

Department of Justice

- 📞 (+632) 8523-8481 to 98
- 📘 www.facebook.com/dojphilippines.official/
- 👉 www.doj.gov.ph

Philippine National Police

- 📞 **Emergency Number:** 117
- 📱 **Non-Emergency Contact:** Text PNP (space) (message) send to 2920
- 📞 **Local PNP Helpline:** (02) 8723-0401 loc. 6071 16677
- 👉 www.pnp.gov.ph

Aleng Pulis

- 📞 **Smart:** (+63) 919-777-7377
- 📞 (02) 723-0401
- 📘 www.facebook.com/wcpc.didmpnp

Internet Watch Foundation

- 📞 +44 (0)1223-20-30-30
- ✉️ media@iwf.org.uk
- 👉 www.iwf.org.uk/

#SaferKids PH

- ✉️ rvillafranca@unicef.org
- ✉️ mquezon@unicef.org
- ✉️ mmardivilla@unicef.org

