REPUBLIC OF THE PHILIPPINES

DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

DEPARTMENT CIRCULAR NO. 015 DEC-18-2020
Series of 2020

SUBJECT: PRESCRIBING THE CHILD ONLINE SAFEGUARDING POLICY FOR THE FREE INTERNET ACCESS IN PUBLIC PLACES PROGRAM UNDER REPUBLIC ACT NO. 10929.

WHEREAS, the State recognizes the vital role of communication and information in nation-building;[1]

WHEREAS, the State also recognizes the indispensable role of the private sector, encourages private enterprise, and provides incentives to needed investments;[2]

WHEREAS, the State likewise recognizes the vital role of youth in nation-building and shall promote and protect their physical, moral, intellectual and social well-being;[3]

WHEREAS, Article XV of the 1987 Philippine Constitution mandates the State to defend the rights of children to assistance and special protection against all forms of neglect, abuse, cruelty, exploitation and other conditions prejudicial to their development;[4]

WHEREAS, the 1987 Philippine Constitution recognizes the natural and primary right and duty of parents in the rearing of the youth for civic efficiency and the development of moral character, which natural right and duty of the parents shall receive the support of the Government;[5]

WHEREAS, the United Nations Convention on the Rights of the Child (UNCRC) to which the Philippines is a signatory, mandates State parties to take all appropriate measures to protect children from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse, while in the care of parent(s), legal guardian(s), or any other person who has the care of the child,[6] and requires the State to ensure that children have access to information and material from a diverse selection of national and international sources, especially those aimed at the promotion of his or her social, spiritual and moral well-being and physical health, and to encourage the development of appropriate guidelines for the protection of children from any information and material injurious to their well-being;[7]

WHEREAS, General Comment No. 13 of the UNCRC recognizes that children are users of Information and Communications Technology (ICT),[8] that child protection risks exist in relation to ICT,[9] and that there is a need to protect children from perpetrators of violence;[10]

---

[1] II Phil.Const. §24 (1987); RA 10844 §2(a).
[2] II Phil.Const. §20 (1987).
[3] II Phil. Const. §13 (1987).
[4] XV Phil. Const. § 3(2) (1987).
[5] II Phil. Const. §12 (1987).
[6] Art. 19(1) Convention on the Rights of the Child https://www.ohchr.org/en/professionalinterest/pages/crc.aspx.
[7] Art. 17 Convention on the Rights of the Child https://www.ohchr.org/en/professionalinterest/pages/crc.aspx.
[8] UN Committee on the Rights of the Child (CRC). General comment No. 13 (2011): The right of the child to freedom from all forms of violence, Page 12, https://www.refworld.org/docid/4e6da4922.html.
[9] UN Committee on the Rights of the Child (CRC). General comment No. 13 (2011): The right of the child to freedom from all forms of violence, Page 11, https://www.refworld.org/docid/4e6da4922.html.
[10] UN Committee on the Rights of the Child (CRC). General comment No. 13 (2011): The right of the child to freedom from all forms of violence, Page 13, https://www.refworld.org/docid/4e6da4922.html.

WHEREAS, Republic Act (RA) No. 10844, otherwise known as the "*Department of Information and Communications Technology (DICT) Act of 2015,*" declares that it is the policy of the State to empower, through the use of ICT, the disadvantaged segments of the population;[11]

WHEREAS, RA 9775, otherwise known as the *"Anti-Child Pornography Act of 2009,"* declares the policy of the State to guarantee the fundamental rights of children from all forms of neglect, cruelty and other conditions prejudicial to their development, protect children from all forms of exploitation and abuse, and comply with international treaties concerning the rights of children, to which the Philippines is a signatory or a State party;[12]

WHEREAS, Presidential Decree (PD) No. 603, otherwise known as *"The Child and Youth Welfare Code,"* defines the rights and responsibilities of children, and the corresponding authority and obligations of their parents, guardians, community, and the government towards them;

WHEREAS, PD 603 likewise provides that every child has the right to protection against exploitation, improper influences, hazards, and other conditions or circumstances prejudicial to his or her physical, mental, emotional, social and moral development;[13]

WHEREAS, RA 7610, otherwise known as the "*Special Protection of Children Against Abuse, Exploitation and Discrimination Act*," declares the policy of the State to protect children gravely threatened or endangered by circumstances which affect or will affect their survival and normal development over which they have no control;[14]

WHEREAS, RA 9262, otherwise known as the *"Anti-Violence Against Women and Their Children Act of 2004,"* declares the policy of the State to value the dignity of women and children, guarantee full respect for human rights, and protect the family and its members particularly women and children, from violence and threats to their personal safety and security;[15]

WHEREAS, RA 9995, otherwise known as the *"Anti-Photo and Video Voyeurism Act of 2009,"* prohibits the non-consensual taking of photos or video coverage,[16] as well as the copying, reproduction,[17] selling, distributing,[18] publishing, or broadcasting[19] of photos, videos, or any other material containing recordings of sexual acts or similar activities through any means, including Video Compact Disc (VCD), Digital Versatile Disk (DVD), Internet, cellular phones and other similar means or devices;[20]

WHEREAS, RA 10175, otherwise known as the *"Cybercrime Prevention Act of 2012,"* provides for higher penalties for unlawful or prohibited acts defined and punishable under RA 9775, when committed through a computer system;[21]

WHEREAS, RA 10364, otherwise known as the *"Expanded Anti Trafficking in Persons Act of 2012,"* declares it unlawful for any person, natural or juridical, to adopt persons by any form of consideration for exploitative purposes or to facilitate the same for purposes of prostitution, pornography, sexual exploitation, forced labor, slavery, involuntary servitude or debt bondage;[22]

---

[11] §2(k), RA 10844.
[12] §2, RA 9775.
[13] Art. 3(8), P.D.603, as amended.
[14] Art.1 RA 7610 §2.
[15] §2, RA 9262.
[16] §4(a) RA 9995.
[17] *Id.* at §4(b).
[18] *Id.* at §4(c).
[19] *Id.* at §4(d).
[20] §4, RA 9995.
[21] §4(c)(2), RA 10175.
[22] §4(f) RA 10364.

WHEREAS, it is in the public interest and the general welfare that policy interventions be instituted to address disadvantages and prevent potential risks and hazards of Internet connectivity, thereby allowing the nation's children to enjoy the full benefits and advantages, thereof as an effective means for communication and access to useful, meaningful, and relevant data and information;

WHEREAS, the implementation and use of the free public Internet ought to provide effective safeguards against its unchecked and irresponsible use so that bullies, sex offenders, traffickers, and persons who harm children are prevented from abusing the free public Internet to contact potential victims, to share content and images of their abuse, and to encourage others to commit further crimes;[23]

WHEREAS, the integration of child-friendly policies and processes into the core strategies and models employed by the private and public sectors can effectively address the different ways their various operations can impact children, strengthen their social license to operate, and complement the duty of the State to protect children's rights;

WHEREAS, Presidential Proclamation No. 731 s. 1996 declares the second week of February, every year, as the "National Awareness Week for the Prevention of Child Sexual Abuse and Exploitation;"

WHEREAS, RA 10929, otherwise known as the *"Free Internet Access in Public Places (FIAPP) Act,"* states that the Department of Information and Communications Technology (DICT), in coordination with the Inter-Agency Council Against Child Pornography (IACACP), and in consultation with telecommunications companies and civil society organizations, shall develop standards and mechanisms for the protection of children online, consistent with existing laws on the rights and protection of the welfare of children;[24]

WHEREAS, under the FIAPP Program, technical solutions that may limit or restrict access shall only be employed when there is clear and present technical risk or breach that cannot be remedied through ordinary technical solutions; *Provided*, that technical solutions that can likewise maintain or promote ease of access shall be prioritized and pursued;[25]

WHEREAS, the free Internet access provided under the FIAPP Act is a public service administered and implemented by the government,[26] access to and the use of which may be subjected to necessary and reasonable regulation and monitoring in order to enhance the government's ability to ensure cybersecurity, combat illegal cyber activities,[27] safeguard data privacy, and prevent the aforesaid free public service from being misused in an illegal or unacceptable manner;

WHEREAS, RA 10929 expressly prohibits access to pornographic websites under the FIAPP Program;[28]

---

[23] UNICEF. State of the World's Children 2017: Children in a Digital World, page 71. Anonymity likewise reduces their risk of identification and prosecution, expands their networks, increases profits, and enables them to pursue many victims at once.

[24] §11, RA 10929.

[25] §3(c), RA 10929.

[26] §5, RA 10929.

[27] *See Disini v. Secretary of Justice*, G.R.No. 203335, February 11, 2014 (En Banc), to wit: "Undoubtedly, the State has a compelling interest in enacting the cybercrime law for there is a need to put order to the tremendous activities in cyberspace for public good. To do this, it is within the realm of reason that the government should be able to monitor traffic data to enhance its ability to combat all sorts of cybercrimes. xxx. There are many ways the cyber criminals can quickly erase their tracks. Those who peddle child pornography could use relays of computers to mislead law enforcement authorities regarding their places of operations. Evidently, it is only real-time traffic data collection or recording and a subsequent recourse to court-issued search and seizure warrant that can succeed in ferreting them out."

[28] §10, RA 10929.

WHEREAS, under RA 10844, the DICT is the primary policy, planning, coordinating, implementing, and administrative entity of the Executive Branch of the government that will plan, develop, and promote the national ICT development agenda;[29]

WHEREAS, RA 10844 empowers the DICT to ensure and protect the rights and welfare of consumers and business users to privacy, security and confidentiality in matters relating to ICT, in coordination with the agencies concerned, the private sector and relevant international bodies;[30]

WHEREAS, RA 10844 authorizes the DICT to formulate, recommend, and implement national policies, plans, programs, and guidelines that will promote the development and use of ICT with due consideration to the advantages of convergence and emerging technologies;[31]

WHEREAS, the DICT Secretary is authorized by law to formulate such rules and regulations, and exercise such other powers as may be required to implement the Department's statutory objectives;[32]

NOW, THEREFORE, in view of the foregoing, in the exigency of the service, pursuant to RA 10844, RA 10929, and other existing laws, this Circular is hereby issued to institutionalize the **CHILD ONLINE SAFEGUARDING POLICY FOR THE FREE INTERNET ACCESS IN PUBLIC PLACES PROGRAM**, *to wit*:

I.
GENERAL PROVISIONS

Section 1. Purpose.—This Department Circular is being issued to prescribe the guidelines, mechanisms, and standards to promote the safeguarding and protection of children and youth online in the implementation of the FIAPP Program under RA 10929.

Section 2. Coverage.—This Circular shall cover all public places in which the FIAPP Program is implemented. It shall likewise apply to all stakeholders, inclusive of NGAs, LGUs, SUCs, CSOs, NGOs, and private entities, such as ISPs, telecommunications service providers, among others, that participate in the FIAPP Program, or whose products and services are accessible through the FIAPP Program.

Section 3. Definition of Terms.—For purposes of this Circular, the following terms are defined, *to wit*:

a. **"Allow List"** refers to the DICT-curated list of software, domains, or network addresses which are deemed safe to access *via* the 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.

b. **"Authority"** or **"Authorities"** refers to the government agency or agencies in charge of law implementation and enforcement, including but not limited to the 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.

---

[29] §5, RA 10844.
[30] *Id.* at §6(IV).
[31] *Id.* at §6(l)(a).
[32] *Id.* at §8(k).

c. **"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."

d. **"CHED"** refers to the Commission on Higher Education.

e. **"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.[33]

f. **"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 (i) exposes children to scams, identity theft, pornography, explicit content, hate speech, harassment, discrimination, cybercrimes, or other similar activities; (ii) encourages children to do unnecessary harm or violence upon themselves or to other persons; or (iii) 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.

g. **"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,[34] 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: (i) a person, regardless of age, is presented, depicted, or portrayed as a child; or (ii) a computer-generated, digitally or manually crafted image or graphics of a person is represented or made to appear as a child.[35]

h. **"Child sexual exploitation material"** refers to materials depicting child sexual abuse, sexualized content depicting children, and other similar lewd materials.[36]

i. **"CICC"** refers to the Cybercrime Investigation and Coordinating Center, an agency attached to the DICT.

j. **"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.

k. **"CSOs"** refer to civil service organizations.

l. **"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.

---

[33] §3(a), RA 9775.
[34] *Id.*, §3(b).
[35] *See id.* at §3(a).
[36] *See* Interagency Working Group on Sexual Exploitation of Children (2016), "Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse" (hereinafter Luxembourg Guidelines). Retrieved from: http://luxembourgguidelines.org/.

m. **"Deny List"** 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 Deny List may be accessed through the FIAPP Program.

n. **"DepEd"** refers to the Department of Education.

o. **"DICT" or "Department"** refers to the Department of Information and Communications Technology.

p. **"DOJ"** refers to the Department of Justice.

q. **"DSWD"** refers to the Department of Social Welfare and Development.

r. **"FIAPP Act"** refers to RA 10929, otherwise known as the *"Free Internet Access in Public Places Act."*

s. **"FIAPP Program"** refers to the Free Internet Access in Public Places Program under RA 10929 or the FIAPP Act.

t. **"Free public Internet access points"** refers to the access points for the free Internet service under the FIAPP Program deployed in the public places covered by §4 of RA 10929.

u. **"IACACP"** refers to the Inter-Agency Council Against Child Pornography.

v. **"IRR"** refers to Implementing Rules and Regulations.

w. **"ISP"** refers to Internet Service Providers as defined under existing laws, circulars, rules and regulations.[37]

x. **"LGU"** refers to the Local Government Unit.

y. **"NBI"** refers to the National Bureau of Investigation.

z. **"NGAs"** refers to National Government Agencies.

aa. **"NGOs"** refer to Non-Governmental Organizations.

bb. **"NPC"** refers to the National Privacy Commission, an agency attached to the DICT.

cc. **"NTC"** refers to the National Telecommunications Commission, an agency attached to the DICT.

dd. **"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.

ee. **"Online Risks to Children"** are classified into three (3) categories of risks, namely: Content, Contact, and Conduct. (i) Content Risk exists when a child is exposed to child-inappropriate content, such as lewd or explicit images; (ii) 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; and (iii) Conduct Risk

[37] See for example, *id.* at §3(g).

exists when a child behaves or tends to behave in a way that directly contributes towards Content or Contact Risk.

ff. **"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.

gg. **"Person"** refers to any individual, partnership, corporation, trust, estate, cooperative, association, or other entity, whether natural or juridical.

hh. **"Peer-to-Peer Exchange"** refers to an exchange of information or content using a peer-to-peer network.

ii. **"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.

jj. **"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.[38]

kk. **"PNP"** refers to the Philippine National Police.

ll. **"PNP-ACG"** refers to the PNP Anti-Cybercrime Group.

mm. **"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.

nn. **"Safeguarding"** refers to putting precautionary systems, mechanisms, stipulations, devices, technologies, or other similar protective measures in place in order to prevent or mitigate unwanted or harmful incidents.

oo. **"SUCs"** refers to State Universities and Colleges.

pp. **"TESDA"** refers to the Technical Education and Skills Development Authority.

qq. **"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**.

rr. **"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.

[38] §4(g), RA 10173.

II.
GUIDELINES ON
CHILD ONLINE SAFETY AND PROTECTION

Section 4. Regulating the Use of Free Public Internet.—The access to, and use of, the free public Internet under the FIAPP Program, being a public service of the government, shall be subject to necessary and reasonable regulation and restriction pursuant to applicable laws, policies, guidelines, circulars, rules, regulations, and other relevant departmental issuances.

Section 5. Guiding Principles on Child Online Protection under the FIAPP Program.—The following general guidelines for child online safeguarding shall be observed by all stakeholders, users, beneficiaries, and participants in the FIAPP Program relative to the provisioning of free Internet and use of FIAPP internet access points:

a. The FIAPP Program and its implementation shall be guided by the principles of respecting and protecting children, and teaching them safe online behavior and Responsible Digital Citizenship.

b. The best interest and welfare of the child shall be the primary consideration in all decisions affecting children.

c. Considerations for children's rights, and the relevant safeguarding measures thereon, shall be integrated as part of the FIAPP Program implementation with the aim of identifying, preventing, mitigating, and where appropriate, remediating potential or actual adverse risks and impacts upon children.

d. Access to harmful or child-inappropriate content by children shall be prohibited under the FIAPP Program.

e. Access to pornographic websites shall be prohibited under the FIAPP Program.

f. All child protection laws shall be strictly observed. Any suspected, threatened, or actual violation of child protection laws must be reported immediately to the proper authorities for their appropriate action.

g. Data Privacy Laws, and other applicable laws, circulars, standards, rules and regulations for the protection and security of data shall be strictly followed with regard to the personal information of children. Unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children shall be prohibited relative to the use of the free public Internet under the FIAPP Program.

h. All stakeholders, users, and participants of the FIAPP Program shall be encouraged to actively participate in raising awareness and education on the proper use of the Internet.

i. The free public Internet shall be utilized responsibly and productively as a valuable source of data, information and knowledge, as well as an efficient and effective means for communication and expression.

j. The use and provisioning of technical measures, such as but not limited to, parental control, age verification, and other similar tools, solutions, systems, processes or mechanisms for restricting the child's exposure to illegal or child-inappropriate content *via* the free public Internet shall be effectively implemented in accordance with law.

k. The topic of child online safeguarding under the FIAPP Program shall at all times be subject to the provisions of the COSP, and such other circulars, orders, guidelines, directives, rules and regulations issued by the Department.

Section 6. The Primary Right and Duty of Parents; Collective Cooperation Towards Online Child Safeguarding.—Child online safeguarding measures shall be adopted under the FIAPP Program in support of the natural and primary right and duty of parents in the rearing of the youth for civic efficiency and the development of moral character.[39]

All stakeholders, users, content providers, participants, parents, all members of the community, and beneficiaries of the FIAPP Program shall work together and actively cooperate to ensure that the children's online experiences as users of free public Internet are safe and positive, through initiatives that include the following activities:

a. Making available the appropriate information, references, and other tools, solutions, systems, processes or mechanisms to guide the parents on internet safety, keeping the children safe online, and teaching children responsible digital citizenship.

b. Strongly encouraging parents to take an active role in their children's internet activities, by teaching their children safe and responsible digital citizenship, and by establishing family rules for how, when, and in what manner the Internet should be responsibly used.

c. Fostering and adopting systems, mechanisms, and procedures for proper age verification and prior parental permission for any recorded online interaction, session, transaction or activity involving children, regardless of whether the same is on a one-on-one or group basis.

d. Educating the public and alerting them to Online Risks to Children, such as but not limited to sexual exploitation, self-harm and graphic violence, cyberbullying, cybercrime, and other types of online abuse and child-inappropriate content.

e. Making online safety resources to address Online Risks to Children available and more accessible to the public.

f. Educating and informing parents on how to effectively handle, and report when necessary, the harmful contacts, conduct, and content that are inimical to their children's welfare.

Section 7. Participation in Public Awareness Campaigns.—All stakeholders, users, content providers, participants, parents, members of the community, and beneficiaries of the FIAPP Program, as well as concerned CSOs and NGOs, are strongly encouraged to cooperate and actively participate in all local and international public awareness campaigns for the safeguarding and protection of children online.

The DICT, its central and regional offices and units, as well as its attached agencies, shall (a) spearhead the conduct of government-led public awareness campaigns for the safeguarding and protection of children online across the country; (b) render, within the framework of existing laws, circulars, rules, and regulations, such assistance as may be appropriate to private sector initiatives for effectively raising public awareness on child online safety; and (c) plan, implement, and sustain initiatives, as well as coordinate and collaborate with the IACACP to support the meaningful observance of the "Safer Internet Day for Children Philippines" under Proclamation No. 417 s. 2018, the "National Awareness Week for the Prevention of Child Sexual Abuse and Exploitation" declared under Proclamation No. 731 s. 1996, and other similar events and activities, whether at the local, national, or international level.

---

[39]II Phil.Const. §12 (1987).

Section 8. Unacceptable Uses.—The free public Internet provided under the FIAPP Program shall not be utilized in any manner that is unacceptable. Unacceptable uses thereof shall include but not be limited to the following:

a. Accessing, uploading to, downloading from, sharing, or utilizing pornographic websites.[40]

b. Accessing, uploading to, downloading from, sharing, or utilizing sites that contain child-pornography or other child-exploitative materials.

c. Accessing any material or content that is illegal, or otherwise illegally obtained, inclusive of viewing, downloading, uploading, or making available to other parties any content or material that is illegal or illegally obtained, or otherwise protected by intellectual property laws, without the permission of the owner thereof.

d. Sending or disseminating discriminatory, threatening, or harassing messages to other people in violation of applicable laws, circulars, rules, and regulations.

e. Using the free public Internet, in any manner, that harms or endangers the well-being of a child, or exposes the latter to child-inappropriate content or Online Risks to Children.

f. Hacking, phishing, spamming, cyber-bullying, libel, or any other use that is violative of other people's privacy and other rights under existing laws.

g. Using or inciting others to use the free public Internet access for illegal gambling, the commission of cybercrimes, and other offenses in violation of applicable laws, rules, and regulations.

h. Using the free public Internet in any other manner that is contrary to existing laws, orders, circulars, rules, and regulations.

The DICT, NTC, and/or participating ISPs shall institute, or cause to be instituted, such measures as may be necessary, such as but not limited to the use of appropriate tools, solutions, systems, processes or mechanisms, to effectively enforce the restrictions against unacceptable uses of the free public Internet.

Section 9. Signages.—Government agencies, establishments, schools, and educational institutions that own, operate, administer, or manage the public places in which free public Internet access is made available under the FIAPP Program shall provide and display permanent or semi-permanent signages that are legible, prominent, and visible in the aforesaid public places for purposes of effectively informing the public about:

a. The specific locations within the vicinity where free public Internet is available for access;
b. References to the behavioral protocols and terms of use relative to the free public Internet;
c. Reminders on safe online behavior, and responsible digital citizenship;
d. Warnings and advisories on child online safety and cyber security;
e. Such other public advisories and signages as may be directed in accordance with the FIAPP Program and related departmental policy issuances.

In accordance with §7, Art. XIV of the 1987 Philippine Constitution, the signages shall be in Filipino or English as the official languages of the Philippines. Whenever applicable, accurate translations

[40] *See* §10, RA 10929.

in the local dialect or regional language shall be provided in addition to the official language used on the signages.

The DICT may require that non-compliant signages be taken down or otherwise rectified in order to avoid potential confusion or misinformation relative to the FIAPP Program. To ensure compliance and accuracy of the signages, the concerned agencies and institutions may consult with the Department.

Section 10. DICT-Curated Lists.—Access or use of the free public Internet under the FIAPP Program shall be subject to strict compliance with the DICT-curated Lists instituted under applicable departmental policies issued pursuant to existing laws, orders, circulars, rules, regulations, and relevant departmental issuances, inclusive of the following:

a. ***Deny List.***—The DICT shall develop and maintain, or cause to be developed and maintained, a central database of all sites and domains that are on its Deny List under the FIAPP Program. For this purpose, and to ensure that its Deny List is current and regularly updated, the Department shall regularly coordinate and/or collaborate with the IACACP members, local and international CSOs, NGOs, and other entities. Access to and use of the free public Internet for viewing any site or domain covered by the Deny List shall be prohibited.

b. ***Allow Lists.***—The DICT shall develop and maintain, or cause to be developed and maintained, an Allow List(s), which the Department may prescribe in relation to the access and use of the FIAPP Internet access points within the public educational institutions and learning centers.

    1. For the public basic educational institutions, the Department may coordinate with the DepEd, school administrators, and other concerned stakeholders thereof, for purposes of ensuring that the appropriate Allow List is current and regularly updated.

    2. For SUCs, the Department may coordinate with the CHED, school administrators, and other concerned stakeholders thereof, for purposes of ensuring that the appropriate Allow List is current and regularly updated.

    3. For public learning centers and institutions with children among their beneficiaries, the Department may coordinate with the TESDA or other government agency having jurisdiction thereof, the administrators, and other concerned stakeholders, for purposes of ensuring that the appropriate Allow List is current and regularly updated.

    Access to and use of the free public Internet under the FIAPP Program deployed in public educational institutions and learning centers for viewing any site or domain not covered by the Allow List shall be restricted. In no case shall the Allow List include within its coverage any site or domain listed in the Deny List.

The DICT may institute such measures as may be necessary, through the use of appropriate tools, solutions, systems, processes or mechanisms, inclusive of ensuring the automatic logging out or the imposition of access restrictions for users who attempt to view any of the prohibited or restricted sites or domains, for purposes of strictly implementing the curated lists established under the auspices of the COSP.

Section 11. Bandwidth Management and Access Restrictions on the Free Public Internet.—The DICT shall implement effective systems or mechanisms for bandwidth management to ensure the efficient, effective, and equitable provisioning of bandwidth for the free public Internet access under the FIAPP Program.

For public educational institutions under the FIAPP Program, the DICT may likewise restrict access to the free public Internet, in accordance with the educational institutions' hours of operation, or such other complementary school policies as may be submitted by the administrators thereof to the Department for consideration.

The use of VPNs in accessing the free public Internet under the FIAPP Program shall not be allowed, except when the user can justify, in writing, to the satisfaction of the Department that the particular VPN does not enable access to any illegal content, or unacceptable use under §8 of this Circular.

The DICT, NTC, and/or participating ISPs shall institute, or cause to be instituted, such measures as may be necessary, such as but not limited to the use of appropriate tools, solutions, systems, processes or mechanisms for filtering and blocking as mandated or otherwise authorized by law, to effectively implement the access and other restrictions on the free public Internet under the provisions of this Circular and other existing laws and departmental issuances.

Section 12. Child-Friendly Reporting Mechanisms.—The DICT shall coordinate with all concerned agencies for the development of effective and child-friendly online reporting procedures, systems, and mechanisms.

The reporting procedures, systems, and mechanisms to be instituted shall be simplified and streamlined in such a manner as to ensure that: (a) the information to be required from the reporting party shall be basic and limited only to those that are necessary and required by law, and (b) the reported incidents are, as far as practicable, immediately transmitted within twenty-four (24) hours to the appropriate law enforcement agencies for their proper action.

The reporting procedures, systems, and mechanisms shall, as far as practicable, be made available for ready access *via* diverse traditional and ICT-enabled platforms and avenues, inclusive of internet-based form reporting, hotlines from government agencies and authorities, and such other means as may be instituted or put in place by the IACACP, its members, the LGUs, and other concerned government agencies or instrumentalities.

The reporting procedures, systems, and mechanisms shall be regularly disseminated, published, and promoted in the websites of the DICT and other concerned government agencies, in print and other forms of media, the DICT Child Online Protection website, the Captive Portal, as well as through signages in the public places where free public Internet access is made available under the FIAPP Program.

Section 13. Flagging, Notice, and Take Down.—The DICT, in coordination with the NTC, the telecommunications companies, and the ISPs participating in the FIAPP Program, shall ensure that effective systems, mechanisms, steps, or procedures are instituted in order that illegal, harmful, pornographic, or child-inappropriate content, material, sites, or domains that are accessible through the free public Internet are promptly identified, flagged, and immediately subjected to appropriate processes for notice, take down, and blocking within the framework of applicable laws, orders, circulars, rules and regulations.

Section 14. Supplemental, Complimentary, and Additional Measures.—The Department may institute such additional measures, systems, or mechanisms as may be necessary to effectively perform its mandate as the lead implementing and administering agency for the effective and efficient implementation of RA 10929.

III.
SAFEGUARDING CHILDREN AGAINST UNFAIR OR DECEPTIVE ACTS OR PRACTICES ON WEBSITES OR ONLINE SERVICES ACCESSIBLE THROUGH THE FREE PUBLIC INTERNET

Section 15. Regulation of Unfair or Deceptive Acts or Practices in Relation to the Collection, Use, or Disclosure of Personal Information from and about Children on Websites and Online Services Accessible through the Free Public Internet.—Any person who operates an online service, domain or web site located on the Internet, and who collects or maintains personal information from or about the users of or visitors of such online service, domain or web site, or on whose behalf such information is collected or maintained, or offers products or services for sale through that online service, domain or website, where such online service, domain or web site may be accessible through the free public Internet under the FIAPP program, shall:

a. Provide notice on its online service, domain or web site, of what type of information it collects from children, how it uses such information, and its disclosure practices thereon;

b. Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children;

c. Provide reasonable means for the parent to (i) review the personal information collected from the child, and (ii) refuse permission on the further use or maintenance of such information;

d. Not condition a child's participation in a game, the offering of a prize, or any other activity on the child, upon the child's disclosure of more personal information than is reasonably necessary to participate in such activity; and

e. Establish and maintain such other reasonable procedures as may be necessary to effectively protect the confidentiality, security, integrity, and privacy of personal information collected from children in strict accordance with Data Privacy Laws.

IV.
CHILD ONLINE PROTECTION WEBSITE AND CAPTIVE PORTAL

Section 16. Child Online Protection Website.—The DICT shall develop, or cause to be developed, a website primarily dedicated to Child Online Protection, which shall be presented in a child-friendly language and format. The contents of the Child Online Protection website shall complement the official DICT website, and shall contain relevant and up-to-date educational materials, information, and other online resources on the following subject matters:

a. Basic data and information on child online safety, including its status in the Philippines, and the current Child Online Protection landscape;
b. The importance of maintaining the privacy of the child's personal information;
c. Responsible digital citizenship;
d. Anti-Cyber Bullying;
e. Anti-Child Pornography;
f. Anti-Online Risks to Children;
g. Safeguarding and protecting against online sexual exploitation of children, harmful or child-inappropriate content, and other Online Risks to Children;

h. The threats attendant to online sexual exploitation of children, harmful or child-inappropriate content, and other Online Risks to Children, the ways to prevent exposure to them or to mitigate their effects, and the remedies available to the parent or the child;
i. Current links to online resources from the DICT and its partner government agencies, as well as links to other DICT-curated online resources from the public and private sectors, on the subject of safeguarding and protecting children online;
j. Strategies, mechanisms, and procedures employed by the government to combat child pornography, cybercrime, and other Online Risks to Children;
k. Relevant laws, policies, rules, and regulations on the safeguarding and protection of children online;
l. Other content as may be reasonably necessary, desirable, or incidental in relation to the foregoing matters, or as may be directed by the Department Secretary or his/her duly designated supervising official.

Section 17. The Captive Portal for the FIAPP Program.—The DICT shall pursue and integrate its initiatives for child online safety and protection in the Captive Portal for all free public Internet access points under the FIAPP Program. As the initial web page displayed to end-users who connect to any free public Internet access point covered by the FIAPP Program, the Captive Portal shall require all end-users of the free public Internet to view and interact with it prior to being allowed broader access to the Internet.

The Captive Portal for the FIAPP Program shall require all users to undergo proper age verification. For children using the free public Internet in educational institutions, SUCs, and learning centers, the child's Learners Reference Number or its equivalent shall be logged in or registered in the Captive Portal, prior to the child being given broader access to the Internet. For children using the free public Internet in the public places other than educational institutions, SUCs, and learning centers, the Captive Portal shall require that the name, contact details, and a copy of a government-issued ID or other equivalent documentation of the parent or person exercising parental responsibility over the child be logged in or registered prior to the child being given broader access to the Internet.

Section 18. Reporting Links.—The Child Online Protection website and the Captive Portal shall provide, continuously update, and prominently display, the appropriate reporting links to the Authorities, such as the DICT, DOJ, DSWD, DepEd, PNP, NBI, and other government agencies charged with law enforcement and implementation.

The reporting links and the processes therein shall, as far as practicable, be presented in a child-friendly format. They shall likewise provide the user with the option of either reporting online or through a hotline.

Section 19. Informative Messages or Preventive Warnings.—Informative messages or preventive warnings on the safety and protection of children shall be regularly published and updated in the Child Online Protection website and the Captive Portal, for their proper dissemination to parents, students, and other users of the free public Internet under the FIAPP Program.

a. Messages, warnings, notifications, or embedded links shall be placed in the Child Online Protection website, as well as in the Captive Portal or in the web page or pages immediately thereafter.

b. Messages, warnings, notifications, or embedded links that refer to the protection of the children's rights and basic information on child online protection shall, as far as practicable, use phraseology that can be readily understood by its intended audience, and be presented in the form of short videos, infographics, pop-up messages, or other similar child-friendly formats.

c. Effective measures shall be taken to ensure that the informative messages or preventive warnings are read or viewed by users. Such measures shall include, but not be limited to, ensuring that (i) the messages or warnings are brief, straightforward, conspicuously presented, legible, and readily understood, (ii) questions are answered at the end of the

messages or warnings, (iii) video messages or warnings are continuously played, or (iv) click-through mechanisms are effectively used. The use of any combination of the foregoing, or the use thereof with other similar measures, may likewise be employed.

The informative messages under this Section shall include, but not be limited to, information and resources on the following topics or subject matter: (i) responsible digital citizenship, (ii) the positive use of the Internet for children and Online Child Safety Zones; (iii) the Online Risks to Children, and how to identify, prevent or mitigate them; (iv) proper online behavior and etiquette such as, but not limited to, respecting other users' privacy, verifying facts before posting, not sharing confidential and/or personal information online, and not overloading the free public Internet access system with unnecessary or undesirable files or data; (v) the basic features and use of the Captive Portal and its log-in registration system; (vi) appropriate notices and the purpose for collecting any personally identifiable data or information, consistent with Data Privacy Laws; (vii) the procedures for reporting incidents of violations of the COSP and other relevant laws, circulars, rules and regulations for the safeguarding and protection of children and their rights; and (viii) other information as may be reasonably necessary, desirable, or incidental in relation to the foregoing matters, or as may directed by the Department Secretary or his/her duly designated supervising official.

Section 20. Use of Child-Friendly Format and Official Language in the Child Online Protection Website and the Captive Portal.—The Child Online Protection website and the Captive Portal, and their content, shall be presented in a child-friendly manner, and shall, in accordance with §7, Art. XIV of the 1987 Philippine Constitution, be made available in Filipino or English as the official languages of the Philippines. Whenever applicable, accurate translations in the local dialect or regional language shall likewise be made available in addition to the official languages.

Subject to the availability of departmental resources and appropriate technology, the Department shall endeavor to develop, or cause to be developed, the appropriate online features to offer users the option of having the Child Online Protection website, the Captive Portal, or any of their content presented in Filipino, English, or the local dialect.

V.
ROLES AND RESPONSIBILITIES OF THE DICT AND ITS ATTACHED AGENCIES

Section 21. Department of Information and Communications Technology.—The DICT shall have the following roles and responsibilities:

a. Formulate and pursue programs, policies, standards, and guidelines for the safeguarding and protection of children online, and for the more effective implementation of the COSP;

b. Ensure that the use of the free public Internet is consistent with public policy, compliant with existing laws, circulars, rules and regulations, and in line with current child protection standards and practices, through measures such as but not limited to:

   i. Providing internal guidelines for the identification of domains, network addresses, or websites deemed as either restricted or safe for children;

   ii. Maintaining and regularly updating a database of domains, network addresses, or websites that fall under the DICT-curated lists instituted under §10 of this Circular;

   iii. Determining and prescribing the use of appropriate filtering and blocking tools, solutions, systems, processes or mechanisms to effectively restrict children's access to harmful and age-inappropriate content;

iv. Ensuring the regular inspection of the free public Internet access points in order to monitor the quality of service and compliance with the COSP.

c. Coordinate with and encourage concerned NGAs, LGUs, NGOs and the public to participate and support departmental programs and initiatives on the safeguarding and protection of children online;

d. Assist and provide technical expertise to other government agencies in their development of guidelines for the enforcement and administration of laws, standards, rules, and regulations governing the safeguarding and protection of children online;

e. Foster overall cooperation and coordination by and between all relevant stakeholders for the protection of children online, including but not limited to:

i. International and local public and private subject matter experts and entities, including CSOs and NGOs that generate reports and lists of websites containing child sexual exploitation material, such as the National Center for Exploited and Missing Children (NCEMC) in the United States, the Internet Watch Foundation (IWF) in the United Kingdom, and the International Justice Mission (IJM), and other similar entities;

ii. Stakeholders and operators of root name servers under the Domain Name System (DNS), such as the Internet Corporation for Assigned Names and Numbers (ICANN), and other entities responsible for recording Internet Protocol (IP) addresses of domains and websites containing inappropriate content and preventing them from circumventing the database of Deny List and Allow List;

iii. The Authorities and other law enforcement agencies that have data or information which may be used as evidence for the reporting, notice and take down of abusive and/or illegal materials/content, such as child online sexual exploitation of children, cyberbullying, and the like, as well as for the criminal investigation and prosecution of reported online sexual abuse cases and other crimes or offenses against children.

f. Assist in the development of advocacy campaigns and information dissemination related to the safeguarding and protection of children online, digital hygiene, and responsible digital citizenship, and other similar initiatives;

g. Develop capacity building programs to be implemented among all beneficiary sites to raise awareness on safeguarding and protecting children online, and provide training on prevention, detection, and response to Online Risks to Children and the threats of online child abuse; and

h. Issue such memoranda, orders, guidelines, advisories and other departmental issuances as may be deemed necessary for purposes of effectively implementing the COSP.

Section 22. Roles and Responsibilities of Agencies attached to the DICT.—Consistent with their respective charters, enabling statutes, and applicable administrative relationships with the Department under existing laws, the NTC, NPC, CICC, and such other agencies as may hereafter be attached to the DICT, shall individually and collectively coordinate and cooperate among themselves, with the Department, and with the other relevant Authorities, to ensure the effective implementation and enforcement of all laws, circulars, rules and regulations for the safeguarding and protection of children and their rights online, with the objectives of addressing and effectively suppressing violations in real-time, and ensuring that the violators thereof are apprehended and prosecuted in accordance with law.

The attached agencies shall likewise implement their respective awareness campaign programs on the safeguarding and protection of children online as it relates to their respective agency mandates under existing laws. They shall also conduct monitoring, and provide appropriate assistance upon the request of concerned members of the public or private sector, on matters in which child online safety and their respective jurisdictions coincide.

The attached agencies may issue such supplemental policies, guidelines, and other agency issuances as may be necessary to implement this Section.

VI.
DEPARTMENTAL ASSISTANCE TO OTHER GOVERNMENT AGENCIES

Section 23. General Policy on Providing Technical Assistance to Other Government Agencies.— In accordance with §6(h), RA 10844, and its role as the lead implementing and administering agency in implementing RA 10929, the DICT shall provide such assistance and technical expertise as may be necessary or desirable to other government agencies and instrumentalities in their development of guidelines for the enforcement and administration of laws, standards, rules, and regulations governing the safeguarding and protection of children online, and in the performance of their respective roles and responsibilities under the COSP.

Section 24. Department of Education (DepEd) and the Commission on Higher Education (CHED).—The Department shall, upon request, provide appropriate assistance and technical expertise to the DepEd and CHED in the performance of the latter's mandates under existing laws in connection with the safeguarding and protection of children online, inclusive of but not limited to the following roles and responsibilities:

a. Cooperate and jointly commit to implement the FIAPP Program in public educational institutions and learning centers within their respective jurisdictions in a manner consistent with the COSP and other related laws and regulations on the safeguarding and protection of children online.

b. Develop, in coordination with the DICT and other concerned government agencies:

    i. Informative materials on the COSP, and the requirements of logging in to the free Internet access, for dissemination to all students, their parents, the faculty, and all other staff of schools, offices, or areas under their jurisdiction; and

    ii. The Manual for the COSP and the FIAPP Program, for mandatory use of the school administrators, faculty, staff, personnel, students, and other users in the schools and other public places within their respective jurisdictions.

c. Assist in the dissemination and accessibility of other informative resources and materials on child online protection, such as but not limited to the posting thereof in schools, educational institutions and on their respective websites, and distribution to the students and their parents. Such resources or materials shall, as far as practicable, come from DICT-curated sources, and shall, at the minimum, contain the following:

    i. Basic information on child online protection.

    ii. Information on the standards for online child safety and protection, such as but not limited to the following:

        1. Responsible digital citizenship, and proper behavior on the use of the Internet;

2. Allowable and Unacceptable Uses;
3. Basic features of the registration system and use of the Captive Portal; and
4. Procedures for incident reporting on violations of the COSP and other relevant laws, circulars, rules and regulations for the safeguarding and protection of children and their rights.

d. Ensure the optimal and effective dissemination of the Manual and other information materials mentioned in this section, through the conduct of aggressive information drives, orientation sessions on child online protection in the academic calendar, seminars on child online protection for parents, and other similar initiatives.

Section 25. Department of Social Welfare and Development (DSWD).—The Department shall, upon request, provide appropriate assistance and technical expertise to the DSWD in the performance of the latter's mandates under existing laws in connection with the safeguarding and protection of children online, inclusive of but not limited to the following roles and responsibilities:

a. Formulate protocols for the immediate response, rescue, and debriefing of the victims of online child abuse and other violations of relevant child protection laws, circulars, rules, and regulations.

b. Implement programs pursuant to its mandate under §14 of RA 9775, and other existing laws, in order to ensure that child victims are provided with proper care, custody, and support for their recovery and integration in accordance with existing laws.

Section 26. Authorities and Other Law Enforcement Agencies.—The Department shall, upon request, provide appropriate assistance and technical expertise to the Authorities, including the CICC, NBI, PNP, and other law enforcement agencies in the performance of their respective mandates under existing laws in relation to the safeguarding and protection of children online, inclusive of but not limited to the following roles and responsibilities:

a. Establish protocols and standard operating procedures for gathering digital evidence, and preserving the chain of custody thereof, relative to violations of the COSP and other relevant laws, circulars, rules and regulations for the safeguarding and protection of children online.

b. Establish, maintain, or host appropriate online reporting mechanisms, in addition to other online and offline enforcement processes for the safeguarding and protection of children online.

c. Take appropriate action, investigate, and when necessary, prosecute violations of the COSP and other relevant laws, circulars, rules and regulations for the safeguarding and protection of children online.

d. Cooperate and collaborate with each other with the objective of achieving the more effective enforcement and implementation of the COSP and other related laws on the safeguarding and protection of children online.

Section 27. Department of the Interior and Local Government (DILG).—The Department shall, upon request, provide appropriate assistance and technical expertise to the DILG in the performance of the latter's mandates under existing laws in relation to the safeguarding and protection of children online, inclusive of but not limited to the following roles and responsibilities:

a. Encourage LGUs to formulate and enact ordinances to complement the COSP within their respective jurisdictions.

b. Enter into agreements with concerned agencies for the widespread dissemination and promotion of the COSP.

Section 28. Local Government Units (LGU).—The Department shall, upon request, provide appropriate assistance and technical expertise to the LGUs in the performance of the latter's mandates under existing laws in relation to the safeguarding and protection of children online, inclusive of but not limited to the following roles and responsibilities:

a. Ensure in the enforcement and implementation of the COSP and other laws on the safeguarding and protection of children online within their respective localities;

b. Provide possible configurations of the location-specific content of the Captive Portal, subject to the approval of the DICT as lead implementer of the FIAPP Program, in order to ensure that the Captive Portal and the landing page containing appropriate links to the Child Online Protection Website to be built under Article IV hereof, are prominently visible and accurately translated in the local vernacular;

c. Actively participate in the DICT's capacity building initiatives on content development and standardization on matters relating to the safeguarding and protection of children online, the training of responsible personnel on relevant child online safeguarding protocols; and

d. Assist, where applicable, in formulating accurate translations of the COSP and its related informational resources in the local vernacular.

Section 29. Inter-Agency Council Against Child Pornography (IACACP).—The DICT, in consultation and coordination with the IACACP, shall take appropriate steps to ensure the continuous development and updating of relevant national policies and other information and resources for the safeguarding and protection of children online, and for purposes of effectively addressing online child pornography, the online sexual exploitation of children, and other types of abuses committed against children online.

VII.
CONCERNED PRIVATE SECTORS, OPERATORS AND STAKEHOLDERS

Section 30. Individual and Cooperative Efforts, Pro-active Vigilance among all Private Sector Stakeholders.—The proactive vigilance, as well as the individual and cooperative efforts, of all private sector stakeholders in ensuring due compliance and observance of all child protection laws, circulars, rules and regulations shall be encouraged, the same being integral to the effective safeguarding and protection of children online in their use of the free public Internet under the FIAPP Program.

Section 31. Content Owners.—The owners of content that may be accessed online through the free public Internet under the FIAPP Program shall:

a. Strictly comply with the prohibitions under RA 9775, otherwise known as the *"Anti-Child Pornography Act of 2009;"*

b. Ensure that their content, material, goods or services that are inappropriate for children or otherwise regulated shall be appropriately and prominently marked as such online, and made available only through sites, platforms, or applications that have effective age verification and other related systems, tools, or solutions, and Terms of Use that are compliant with applicable laws, circulars, orders, rules, and regulations on the access, use, possession, sale or distribution of age-restricted or other similarly regulated content, materials, goods and services online;

c. Ensure that content, material, goods or services that are directed at or made suitable for children shall be appropriately and prominently marked as such online, and made available only through sites, platforms, or applications that have effective age verification systems, tools, or solutions, and Terms of Use appropriate thereto, in accordance with all generally applicable laws, circulars, orders, rules, and regulations;

d. As far as practicable, utilize only those online sites, portals, platforms, or applications that promote the safe and secure participation and self-expression of children as Responsible Digital Citizens in the online environment;

e. Strictly comply with the provisions of the COSP and other departmental issuances relating to the implementation of the FIAPP Program;

f. Observe in good faith all applicable laws, circulars, orders, rules, and regulations relating to the safeguarding and protection of children online.

Section 32. Internet Content Hosts.—All persons who host or propose to host internet content that may be accessed through the free public Internet under the FIAPP Program shall:

a. Strictly comply with the prohibitions under RA 9775, as well as with the duties and responsibilities mandated upon all Internet Content Hosts under §11 thereof;

b. Ensure that content that are inappropriate for children, those that are otherwise regulated, or those directed at or made suitable for children shall be appropriately and prominently marked as such, when hosted through their site, portal, platform, or application and made available online;

c. Utilize effective age verification systems, tools, or solutions to ensure strict compliance with the laws, circulars, orders, rules and regulations on the access, use, possession, sale or distribution of age-restricted and other similarly regulated goods and services online;

d. Develop, modify, or upgrade their hosting sites, platforms, or applications, and their Terms of Use thereof, in a manner that ensures and facilitates the content owner's compliance with §31 of this Circular, and effectively promotes the safe and secure participation and self-expression of children as responsible digital citizens in the online environment;

e. Strictly comply with provisions of the COSP and other departmental issuances relating to the implementation of the FIAPP Program;

f. Observe in good faith all applicable laws, circulars, orders, rules, and regulations relating to the safeguarding and protection of children online.

Section 33. Online Business Establishments, Virtual Malls, and Similar Platforms.—All owners/operators/lessors of virtual malls whose websites, portals, systems, applications, or platforms enable the conduct of businesses or other transactions in goods and services online or over the internet, and whose virtual premises may be accessed through the free public Internet under the FIAPP Program, shall:

a. Strictly comply with the prohibitions under RA 9775, as well as with the duties and responsibilities mandated upon all mall owners/operators and owners or lessors of other business establishments under §10 thereof;

b. Ensure that content, material, goods or services that are inappropriate for children, those that are otherwise regulated, or those directed at or made suitable for children, when

accessible online through their virtual malls or premises, shall be appropriately and prominently marked as such;

c. Utilize effective age verification systems, tools, or solutions to ensure strict compliance with the laws, circulars, orders, rules and regulations on the access, use, possession, sale or distribution of age-restricted and other similarly regulated goods and services online;

d. Develop, modify, or upgrade their hosting sites, platforms, or applications, and the Terms of Use thereof, in a manner that ensures and facilitates the content owner's compliance with §31 of this Circular, and effectively promotes the safe and secure participation and self-expression of children as responsible digital citizens in the online environment;

e. Strictly comply with the provisions of the COSP and other departmental issuances relating to the implementation of the FIAPP Program;

f. Observe in good faith all applicable laws, circulars, orders, rules, and regulations relating to the safeguarding and protection of children online.

Owners or operators of virtual malls whose virtual premises may be accessed through the free public Internet under the FIAPP Program shall likewise comply with the provisions of §31 hereof as content owners insofar as their websites, portals, platforms, or applications enable them to conduct transactions involving their own content, materials, goods, or services online.

Section 34. Internet Service Providers (ISPs).—All ISPs, including telecommunications companies engaged in providing internet services, that participate in providing free public Internet as a service under the FIAPP Program shall:

a. Strictly comply with the prohibitions under RA 9775, as well as with the duties and responsibilities mandated upon all ISPs under §9 thereof;

b. Make their Terms of Use available to each user, through a readily identifiable link in the Captive Portal. At the minimum, the Terms of Use shall be compliant with all applicable laws, circulars, rules, and regulations issued by the Authorities, and shall clearly and unequivocally state that:

   i. Any person who uses the service shall be deemed to have read and understood the Terms of Use;
   ii. Any user or account that distributes child pornography or other illegal material, or content that in any manner violates the Terms of Use shall be reported to the Authorities, and other concerned law enforcement agencies for immediate appropriate action;
   iii. There is a minimum user age and/or consent requirement for using the service; and
   iv. The unacceptable uses of the service are prohibited and shall be dealt with in accordance with applicable laws, policies, rules, and regulations.

c. Endeavor to determine harmful websites, in addition to the websites included in the lists curated by the DICT under §10 of this Circular, to which children's access shall be restricted whenever appropriate;

d. Share information about harmful sites to other ISPs and the DICT;

e. Use appropriate Internet filtering software that will effectively limit children's access to unauthorized websites;

f. Put in place internal procedures to ensure compliance with the COSP and other applicable guidelines, rules, and regulations of the DICT on matters relating to child online safety and the use of the free public Internet access points;

g. Strictly comply with provisions of the COSP and other departmental issuances relating to the implementation of the FIAPP Program;

h. Observe in good faith all applicable laws, circulars, orders, rules, and regulations relating to the safeguarding and protection of children online.

Section 35. CSOs and Subject Matter Experts on the Safeguarding and Protection of Children Online.—The CSOs and subject matter experts on the safeguarding and protection of children online shall:

a. Endeavor to complement the Department's information and awareness campaigns, as well as those of the public and private sector, by continuing their advocacy work and trainings aimed at effectively addressing Online Risks to Children, Child Pornography, Responsible Digital Citizenship, Safe and Responsible Internet Use, and the remedial processes available against violations of online child protection laws, circulars, orders, rules, and regulations;

b. Engage with or provide inputs and observations to the NGAs in the latter's formulation of initiatives, policies and programs for the safeguarding and protection of children online, and the responsible use of the free public Internet;

c. Undertake programs and activities, in coordination with other government agencies and instrumentalities, geared towards the prevention, investigation, and prosecution of offenses and abuses committed against children online.

VIII.
FINAL PROVISIONS

Section 36. Enforcement, Investigation, Institution of Appropriate Proceedings.—Without prejudice to the application and enforcement of other applicable laws, circulars, rules, regulations, and other legal processes, the Department may, either *motu proprio* or upon complaint, pursue appropriate enforcement and investigation proceedings upon any violation or circumvention of the provisions of this Circular, with a view towards instituting such civil, criminal, administrative cases, or any combination thereof, as may be warranted pursuant to applicable laws, guidelines, rules, regulations, and other issuances.

In the enforcement, investigation, prosecution, litigation, and other relevant proceedings against violations of the COSP and other online child protection laws, circulars, rules, and regulations, due consideration shall be given to the evidentiary rules provided under existing laws and rules of procedure.[41]

Failure to enforce the strict compliance of this Circular at any time shall not constitute a waiver of the Department's right to subsequently enforce the provisions hereof, neither shall non-compliance of this Circular be considered a sufficient justification against its coverage and application.

The care, custody, treatment, and the right to privacy of the child victim shall be ensured at any and all stages of the litigation, prosecution and trial for violations of RA 9775 and other existing laws, circulars, rules, and regulations for the protection of children online.[42]

---

[41]See for example, last par. §11, RA 9775, to wit: "…Provided, That the failure of the internet content host to remove any form of child pornography within forty-eight (48) hours from receiving the notice that any form of child pornography is hitting its server shall be conclusive evidence of willful and intentional violation thereof."
[42] See §§13-14, RA 9775 cf. RA 6981, RA 7309.

Section 37. Policy Monitoring and Assessment.—The DICT, in coordination and collaboration with all concerned government agencies and stakeholders, shall monitor and assess the implementation of the COSP every two (2) years, or sooner as may be directed by the Department Secretary.

Section 38. Periodic Updating of the COSP.—The DICT shall ensure that the COSP shall be periodically updated to maintain its effectiveness, in light of changes in technology and the ICT environment. For this purpose, it may consult with child online safeguarding experts and other relevant stakeholders.

Section 39. Timeline for Implementation.—Subject to the availability of funds and resources, the Department shall endeavor to forthwith complete and fully operationalize the infrastructure, systems, equipment, goods or services necessary in order to effectively implement the COSP within a reasonable period of time.

Due to the public interest in ensuring the safeguarding and protection of every child from harm on account of the digital environment, the Department shall prioritize the full implementation of the COSP as supported through cost-benefit and results-based plans formulated through cooperation and collaboration with the IACACP, its partners, and the stakeholders.

Section 40. Upgrading of FIAPP Systems and Infrastructure.—Nothing in the COSP or other related departmental issuances shall hinder or prejudice the DICT from updating or upgrading any of its systems and infrastructure for the FIAPP Program at any time, taking into consideration the advances in technology, and relevant developments in the applicable laws and regulatory environment.

Section 41. Reservation Clause.—The Department Secretary shall have the power to amend, modify or revoke the provisions of this Circular, or impose further conditions, as may be necessary in the public interest. Nothing in this Circular shall be construed to limit, decrease, or restrain the Department's authority and mandate under RA 10844, RA 10929, the Revised Administrative Code, and other existing laws, rules, regulations, and issuances.

Section 42. Separability Clause.—If any section or part of this issuance is held unconstitutional or invalid, the other sections or provisions not otherwise affected shall remain in full force and effect.

Section 43. Repealing Clause.—All other issuances or parts thereof that are inconsistent with this Department Circular are hereby repealed or modified accordingly.

Section 44. Effectivity.—This issuance shall take effect fifteen (15) days after its publication in a newspaper of general circulation and upon the filing of three (3) certified true copies thereof with the Office of the National Administrative Register (ONAR), University of the Philippines Law Center.

GREGORIO B. HONASAN II
Secretary