



HOUSE OF REPRESENTATIVES

H. No. 11566

BY REPRESENTATIVES DY (F.), HERNANDEZ (F.), MARCOS, FRESNEDI, MONTES, BENITEZ (J.M.), REVILLA (B.), MERCADO-REVILLA, REVILLA (R.J.), ROMUALDEZ (F.M.), ROMUALDEZ (Y.M.), ROMUALDEZ (A.J.), ACIDRE, DEL MAR, ZUBIRI, MIRAFLORES, LAGBAS, GORRICETA, TUPAS, VILLANUEVA, VELOSO, YAP (C.), YAP (ERIC), SORIANO, EMANO, GALANG, SAN FERNANDO, HERNANDEZ (C.A.), LACSON, DAZA, MERCADO, COLLANTES, GARCIA (K.H.), CRUZ (R.), SUAREZ, ADIONG, LAZATIN, ARENAS, VARGAS, LUISTRO, LEGARDA, LORIA, CATULPOS, CHUA, TEVES, GOMEZ, CHUA-TAI, CAYTON, NAZAL, ORETA, YATCO, SUANSING (M.A.), ROMULO, SINGSON (R.), TAN (K.M.), RIVERA, PUNO, CAGAS, ERICE, LOYOLA, LAGON (S.), BULUT-BEGTANG, CARI, ZAMORA (Y.M.), LEDESMA, PANALIGAN, OLIVAREZ, GONZALES (A.M.), RAMA, AQUINO-MAGSAYSAY, CORVERA, HERNANDEZ (D.), OUANO-DIZON, MATIBAG, ALBA, DAGOOC, AYON, ESPINA, ROQUE, DELOS SANTOS, VILLARICA, LIBANAN, OAMINAL (H.), AGYAO, HOFER-HASIM, CRUZADO, TALLADO, GLEPA, CO-PILAR, BAUTISTA-LIM, ABANTE, GARCIA (A.), BARONDA, LAGDAMEO (M.Y.M.), SAGARBARRIA, POE, LEGAZPI, DALOG, ODUKADO, ESCUDERO, GALEOS, FLORES, DE VENECIA, SINGSON-MEEHAN, BELTRAN, GATCHALIAN, FRASCO, TIANGCO, SALCEDA, VELOSO-TUAZON, CASTRO, GUINTU, PRIMICIAS-AGABAS, DIONISIO, GUTIERREZ, ORTEGA AND KHONGHUN

AN ACT ESTABLISHING SAFETY STANDARDS AND REGULATORY MEASURES TO PROTECT CHILDREN ON SOCIAL MEDIA AND ONLINE GAMING PLATFORMS

*Be it enacted by the Senate and House of Representatives of the Philippines in
Congress assembled:*

CHAPTER I

GENERAL PROVISIONS

SECTION 1. *Short Title.* – This Act shall be known as the “Safe and Friendly Environment for Kids in Digital Spaces (SAFE Kids) Act.”

SEC. 2. *Declaration of Policy.* – It is the policy of the State to recognize the vital role of the youth in nation-building and promote and protect their physical, mental, psychological, moral, spiritual, intellectual, digital, and social well-being. The State likewise affirms its duty to protect children from all forms of neglect, abuse, exploitation, violence, and other conditions prejudicial to their development and uphold their dignity, rights, and best interests.

The State recognizes the vital role of information and communications technology in advancing education, communication, innovation, and national development, while acknowledging that technology presents both opportunities for children's learning, participation, and development and risks to their safety, privacy, health, and well-being.

1 Accordingly, the State shall adopt a rights-based, child-centered, and
2 whole-of-government approach to promote a safe, secure, inclusive, age-appropriate,
3 and developmentally appropriate digital environment for every child. To this end, it shall
4 establish minimum age requirements for access to Digital Platforms; require such
5 Digital Platforms to implement effective child safety, privacy, and accountability
6 measures and adhere to Safety by Design and Safety by Default principles; strengthen
7 digital literacy and responsible digital citizenship; and protect children from online harm
8 while safeguarding their rights to education, access to information, privacy, freedom
9 of expression, and meaningful participation.

10
11 The best interests of the child shall be the primary consideration in the
12 interpretation, implementation, and enforcement of this Act.

13
14 **SEC. 3. Definition of Terms.** – As used in this Act:

- 15
16 (a) **Age Assurance** refers to methods and measures used to determine or
17 reasonably estimate the age or age range of a user, for the purpose of
18 ensuring the application of appropriate age-based protections, while
19 respecting and safeguarding the user's privacy. These may include age
20 verification, age estimation, parental attestation, and other comparable
21 methods;
22
23 (b) **Application Distribution Provider** refers to the platform, marketplace, or
24 intermediary entity responsible for hosting, making available, and delivering
25 software applications to end-users or testers;
26
27 (c) **Artificial Intelligence System** refers to a machine-based system that, for
28 explicit or implicit objectives, infers, from the input it receives, how to generate
29 outputs, such as predictions, content, recommendations, or decisions that can
30 influence physical or virtual environments;
31
32 (d) **Child** refers to a person below eighteen (18) years of age or a person eighteen
33 (18) years of age or over who is unable to fully take care of or protect oneself
34 from abuse, neglect, cruelty, exploitation, or discrimination because of mental
35 or intellectual disability or condition;
36
37 (e) **Child Safety Risk Assessment** refers to a systematic and documented
38 process undertaken by Digital Platforms to identify, analyze, evaluate, and
39 mitigate actual or reasonably foreseeable risks of harm to children arising from
40 the design, operation, features, functionalities, algorithms, Recommender
41 Systems, content, or use of their service. The assessment may include risks
42 arising from exposure to Harmful or Prohibited Content, contact with harmful
43 persons, harmful conduct, exploitation, cyberbullying, grooming, abuse,
44 privacy violations, addictive or compulsive use, and other reasonably
45 foreseeable harms affecting children's safety, health, well-being,
46 development, or rights;
47
48 (f) **Digital Platform** refers to Social Media Platforms, Functionally Equivalent
49 Digital Services, Online Gaming Platforms, Application Distribution Providers,
50 and Operating System Providers subject to and covered under this Act;

- 1 (g) **Functionally Equivalent Digital Service** refers to a digital service that is not
2 nominally a Social Media Platform but performs core social-networking,
3 content-sharing, communication, user-interaction, Livestreaming, or
4 substantially similar functions and presents child online safety risks
5 substantially similar to those addressed under this Act;
6
- 7 (h) **Harmful or Prohibited Content** refers to content that promotes, glorifies,
8 encourages, facilitates, or provides instructions for violence, self-harm, violent
9 extremism, including nihilistic violent extremism and other emerging forms
10 thereof, sexual abuse and exploitation, or other conduct that constitutes a
11 serious and foreseeable risk to the safety or well-being of children, or contains
12 deepfake or synthetic media that realistically simulate, fabricate, modify, or
13 imitate the appearance, voice, likeness, actions, or statements of a real or
14 fictional person, object, or event for the purpose of misinformation;
15
- 16 (i) **Livestreaming** refers to the real-time or substantially real-time transmission
17 or broadcasting of audio, video, or audiovisual content over the internet or
18 through a digital service, whether such transmission is publicly accessible or
19 accessible to a limited group of users;
20
- 21 (j) **Online Gaming Platform** refers to an internet-based service, application,
22 website, or software that enables users to access, participate in, or interact
23 with online games, including services that provide social, communication,
24 content-sharing, Livestreaming, or other interactive features and functionalities
25 in connection with online gaming;
26
- 27 (k) **Operating System Provider** refers to a person or entity that develops,
28 operates, or provides an operating system that controls or manages basic
29 hardware or software functions of a device and enables software applications
30 to run thereon;
31
- 32 (l) **Parental Consent** refers to any freely given, specific, informed, and verifiable
33 agreement by a parent or parent-substitute authorizing an act for which
34 parental consent is expressly required under this Act;
35
- 36 (m) **Parent-Substitute** refers to a person other than the biological parent who has
37 custody over a child and is primarily responsible for the care, and physical,
38 moral, and intellectual development of such child, such as foster care parents,
39 legal guardians, and care providers;
40
- 41 (n) **Parents** refer to biological parents and adoptive parents;
42
- 43 (o) **Recommender System** refers to a fully or partially automated system used
44 by a Digital Platform that suggest, recommend, select, rank, prioritize, curate,
45 or otherwise determine the relative order, prominence, or presentation of
46 specific information or content to a user, including content presented as a
47 result of a search or based on the user's activities, preferences, interactions,
48 or other signals;
49
- 50 (p) **Safety by Default** refers to the automatic application of age-appropriate
51 safety, privacy, and security settings and protections to a child's account or
52 access to a digital service, without requiring the child or parent to activate,

1 configure, or otherwise take affirmative action to obtain such protections,
2 subject to the child's age, developmental capacity, and the risks reasonably
3 associated with the service or functionality;
4

5 (q) **Safety by Design** refers to the systematic incorporation of child safety,
6 privacy, security, and age-appropriate protections into the design,
7 development, configuration, operation, and modification of a digital service,
8 including its features, functionalities, algorithms, Recommender Systems,
9 business practices, and user interfaces, to identify, prevent, mitigate, and
10 address reasonably foreseeable risks of harm to children from the use of such
11 service;
12

13 (r) **Social Media Platform** refers to any internet-based service, network,
14 application, website, or software whose purpose is to facilitate online social
15 networking or allow the creation, sharing, or dissemination of user-generated
16 content. The term shall not include the following:
17

18 (1) Electronic mail services;

19 (2) Short messaging services;

20 (3) Private messaging services without public or discoverable social
21 networking functions;

22 (4) Educational platforms and enterprise, workplace, or professional
23 collaboration tools, approved by the Department of Education (DepEd)
24 or other national government agencies concerned;

25 (5) Digital news services; and

26 (6) Government digital services; and
27

28 (s) **User-generated Content** refers to any information, material, or content
29 created, uploaded, posted, transmitted, shared, streamed, published, or
30 otherwise made available by a user through a digital service, including text,
31 images, photographs, audio, video, livestreams, software, comments,
32 messages, and other forms of digital expression.
33

34 **SEC. 4. Coverage.** – This Act shall apply to all Digital Platforms that are accessible,
35 offered, or made available to users in the Philippines, regardless of their place of
36 incorporation, principal place of business, or location of their servers.
37

38 For purposes of this Act, an Online Gaming Platform shall be covered only with
39 respect to its social, communication, content-sharing, Livestreaming, user-interaction,
40 recommender, or other interactive features and functionalities. Nothing in this Act shall
41 be construed to diminish, exclude, or transfer the existing jurisdiction, regulatory
42 authority, or enforcement powers of the Philippine Amusement and Gaming Corporation,
43 the Games and Amusements Board, the Movie and Television Review and
44 Classification Board, or other competent government agencies over matters within
45 their respective mandates, except to the extent expressly provided in this Act with
46 respect to child online safety risks arising from covered social or interactive
47 functionalities.

Coverage under this Act shall be determined by the Office created under Section 8 herein based on the actual functions, features, and risks of a service, rather than solely on its name, stated purpose, business model, or manner of marketing. The said Office may make a written determination of coverage based on such statutory criteria and standards, subject to notice, due process, and applicable remedies in accordance with this Act.

CHAPTER II

ACCESS OF CHILDREN TO SOCIAL MEDIA

SEC. 5. *Minimum Age Requirement.* – No Social Media Platform, Functionally Equivalent Digital Service, Application Distribution and Operating System Provider, or Online Gaming Platform with respect to its social, communication, content-sharing, Livestreaming, user-interaction, or other interactive features and functionalities, shall allow a person below thirteen (13) years of age to create, register, maintain, or use an account or otherwise access such service or features.

Upon determining or becoming aware that an account is being maintained or used by a person below thirteen (13) years of age, the Digital Platforms shall, without undue delay, disable the account and take reasonable, proportionate, and privacy-preserving measures to prevent its continued use or recreation.

SEC. 6. *Conditional and Risk-Based Access.* – A child who is at least thirteen (13) years of age but below eighteen (18) years of age may access and use Digital Platforms, subject to the restrictions prescribed under this Act. The following contents, features, functions, or practices shall be restricted and not be accessible to such child:

- (a) Harmful or Prohibited Content;
- (b) Advertisements;
- (c) Recommendations;
- (d) Communications and interactions;
- (e) Livestreaming;
- (f) Endless scrolling;
- (g) Short-form video feeds or “shorts”;
- (h) Behavioral profiling;
- (i) Unnecessary collection or sharing of personal information;
- (j) Purchases;
- (k) Gambling-like mechanisms; and
- (l) Other features or practices that may pose reasonably foreseeable and material risks to the safety, health, privacy, development, education, sleep, or well-being of children.

Access to and use of the Digital Platforms under this Act shall be subject to parental consent.

1 Upon determining or becoming aware that an account is being maintained or used
2 by a person within this age range, the Digital Platforms shall, without undue delay,
3 apply the restrictions and safeguards prescribed under this Act to such account.
4

5 Likewise, upon request of parents whose consent was withdrawn, Digital Platforms
6 shall prohibit any access and deactivate the account of a child at least thirteen (13)
7 years of age but below eighteen (18) years of age. Parental consent may be withdrawn
8 anytime, bearing in mind the best interests of the child. Upon request of the parent whose
9 consent was withdrawn, Digital Platforms shall prohibit any access and deactivate
10 the account of a child of at least thirteen (13) years of age but below eighteen (18) years
11 of age.
12

13 **SEC. 7. Age-Appropriate Digital Environment.** – The Digital Platforms shall, within
14 the scope of their respective functions, capabilities, and obligations under this Act,
15 implement reasonable, proportionate, age-appropriate, and technically feasible
16 measures to provide and maintain a digital environment consistent with the age,
17 developmental capacity, safety, privacy, dignity, and best interests of children.
18

19 The measures required under this Act shall be implemented in accordance with the
20 duties, standards, and safeguards prescribed herein and shall not be made dependent
21 upon parental consent, parental supervision, or affirmative action by the child or parent
22 to activate or configure safety protections.
23

24 CHAPTER III

25 IMPLEMENTING AND REGULATORY FRAMEWORK

26 **SEC. 8. Office for Safe and Friendly Environment for Kids in Digital Spaces**
27 **(SAFE Kids Office).** – There is hereby created an Office for Children’s Social Media and
28 Digital Safety, hereinafter referred to as the SAFE Kids Office, within the Department of
29 Information and Communications Technology (DICT).

30 The Office shall be the primary regulatory agency responsible for the
31 implementation and enforcement of this Act within the scope of authority expressly
32 granted herein. The Office shall be under the administrative supervision of the
33 Secretary of Information and Communications Technology and shall exercise such
34 regulatory, compliance, monitoring, and investigative powers expressly granted under
35 this Act.

36 The Office shall coordinate with the Cybercrime Investigation and Coordinating
37 Center (CICC), Department of Justice (DOJ), the National Privacy Commission (NPC),
38 the National Telecommunications Commission (NTC), the Philippine Statistics
39 Authority (PSA), the Philippine National Police, the National Bureau of Investigation,
40 the Council for the Welfare of Children (CWC), and other relevant government
41 agencies to ensure the effective and coordinated implementation of this Act and its
42 harmonization with Republic Act (R.A.) No. 11930 or the “Anti-Online Sexual Abuse or
43 Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation
44 Materials (CSAEM) Act,” and other applicable laws.

45 Nothing in this Act shall be construed to transfer, diminish, or supersede the
46 mandates, powers, and functions of the CICC, DOJ, NPC, NTC, DICT, or other
47 government agencies under existing laws, except as expressly provided in this Act.

1 **SEC. 9. Organization and Staffing of the Office.** – The Office shall be headed by
2 an official designated by the Secretary of Information and Communications
3 Technology.
4

5 The DICT shall determine the organizational structure and staffing pattern of
6 the office subject to the evaluation and approval of the Department of Budget and
7 Management, in accordance with the government optimization program, civil service
8 and other pertinent laws, rules, and regulations.

9 **SEC. 10. Powers and Functions of the Office.** – The Office shall have the following
10 powers and functions:

- 11 (a) Promulgate rules, regulations, standards, and guidelines necessary to
12 implement this Act, in coordination with the DICT, CICC, NTC, NPC, CWC, and
13 other concerned agencies, as appropriate, and subject to applicable laws;
14
- 15 (b) Establish and maintain the regulatory, registration, reporting, monitoring, and
16 compliance framework for Social Media Platforms, Functionally Equivalent
17 Digital Services, Online Gaming Platforms, Application Distribution and
18 Operating System Providers, and other entities expressly covered by this Act;
19
- 20 (c) Establish risk-based, privacy-preserving, and proportionate Age Assurance
21 standards and technical requirements, in coordination with the DICT, NPC,
22 CWC, and other concerned agencies, as appropriate;
- 23 (d) Issue technical standards and guidelines identifying specific forms or
24 manifestations of Harmful or Prohibited Content for purposes of
25 implementation and risk assessments;
26
- 27 (e) Monitor and assess compliance with this Act, its implementing rules and
28 regulations (IRR), and lawful orders or issuances issued pursuant thereto,
29 through inspections, audits, technical assessments, and other appropriate
30 regulatory mechanisms;
31
- 32 (f) Require Digital Platforms to submit information, records, reports, and other
33 documents reasonably necessary to determine compliance, subject to
34 applicable laws, data minimization, confidentiality, and due process;
35
- 36 (g) Issue notices of violation, compliance directives, and corrective or protective
37 measures within its authority under this Act;
38
- 39 (h) Conduct compliance investigations and preliminary investigations into alleged
40 violations of this Act, its IRR, and lawful orders or issuances issued pursuant
41 thereto, gather and evaluate relevant evidence, and refer appropriate cases
42 to the NTC for administrative adjudication, in accordance with law and
43 due process;
44
- 45 (i) Assist the NTC in administrative adjudicatory proceedings by submitting
46 investigation reports, evidence, technical assessments, and other relevant
47 information, without exercising the NTC's adjudicatory authority or determining
48 administrative liability;

- 1 (j) Create, organize, and dissolve inter-agency task forces for specific purposes,
2 as may be necessary for the effective implementation of this Act, and call upon
3 or engage non-governmental organizations, civil society organizations (CSOs),
4 and other relevant stakeholders to provide technical expertise, assistance, and
5 support;
6
7 (k) Coordinate with the DICT, CICC, NTC, NPC, DOJ, CWC, law enforcement
8 agencies, and other concerned government agencies in the implementation
9 and enforcement of this Act;
10
11 (l) Develop programs and initiatives on digital literacy, online safety, responsible
12 digital citizenship, and child protection in the digital environment;
13
14 (m) Conduct or support research, capacity-building, public awareness, and
15 stakeholder engagement concerning children's online safety;
16
17 (n) Periodically review the standards and guidelines on child Safety by Design,
18 Age Assurance, Recommender Systems, algorithmic accountability, artificial
19 intelligence (AI), and other emerging technologies relevant to the protection of
20 children; and
21
22 (o) Perform such other functions as may be necessary to carry out the purposes
23 of this Act.

24 **SEC. 11. NTC Administrative Adjudicatory Jurisdiction.** – Notwithstanding any
25 provision of Executive Order No. 546, s. 1979, as amended, entitled "Creating a
26 Ministry of Public Works and a Ministry of Transportation and Communications," or
27 other laws to the contrary, the NTC shall have original jurisdiction over administrative
28 complaints involving violations of this Act, its IRR, and lawful orders or issuances
29 issued pursuant thereto.

30 For purposes of this Act, the NTC shall have the authority to receive and docket
31 administrative complaints, conduct hearings and administrative proceedings, require
32 the submission of documents and evidence, issue subpoenas in accordance with law,
33 determine administrative liability, impose the administrative penalties provided under
34 this Act, and issue such orders as may be necessary for the proper disposition of
35 administrative cases.

36 The Office shall refer to the NTC administrative complaints and cases within
37 the latter's jurisdiction and shall provide such investigation reports, evidence, technical
38 findings, and other assistance as may be necessary for the adjudication thereof.

39 The exercise of jurisdiction by the NTC under this section shall be without
40 prejudice to the powers and functions of the NPC under applicable data privacy laws,
41 the mandates of other competent government agencies under existing laws, and any
42 civil or criminal liability that may arise from the same act or omission.

1 **SEC. 12. *Inter-Agency Coordination.*** – The Office shall establish mechanisms for
2 coordination among the NTC, NPC, CICC, DOJ, National Security Council,
3 Department of Social Welfare and Development (DSWD), DepEd, law enforcement
4 agencies, and other concerned government agencies for the effective implementation
5 of this Act.

6 The respective powers and functions of government agencies under existing
7 laws shall remain unaffected, except as expressly provided in this Act.

8 **SEC. 13. *Registration and Local Presence.*** – To ensure regulatory accountability
9 and an accessible point of contact for the enforcement of this Act, all Digital Platforms
10 subject to this Act shall comply with the registration and local presence requirements
11 prescribed herein.

12 (a) **Registration and Local Presence.** – Within ninety (90) days from receipt of
13 notice of its coverage under this Act, foreign Digital Platforms shall register
14 with the Securities and Exchange Commission (SEC), where required by
15 applicable law, and shall maintain an accessible local presence in the
16 Philippines through either:

- 17
18 (1) Establishing a domestic corporation duly organized and existing under
19 R.A. No. 11232 or the “Revised Corporation Code of the Philippines”; or
20
21 (2) Registering as a foreign corporation and securing the appropriate license
22 to do business in the Philippines pursuant to R.A. No. 11232, where
23 applicable.

24 A foreign Digital Platform shall maintain a duly authorized local representative
25 or, where required under R.A. No. 11232, a resident agent in the Philippines.
26 The local representative shall serve as the entity’s official point of contact for
27 regulatory matters under this Act, without prejudice to the functions and
28 requirements applicable to a resident agent under R.A. No. 11232.

29 The local representative shall maintain a Philippine address and shall be
30 authorized to receive notices, orders, and other official communications issued
31 by the Office, NTC, or other competent government authorities and to
32 coordinate the compliance and participation of Digital Platforms in
33 administrative proceedings before Philippine authorities. Service of summons
34 and other legal process shall be governed by applicable laws.

35 (b) **Designated Compliance Officer.** – Every Digital Platform subject to this Act
36 shall designate a responsible compliance officer who shall coordinate
37 compliance with this Act and shall have sufficient authority, competence, and
38 resources to perform such functions. The compliance officer shall be a
39 resident of the Philippines.

40
41 The Office may, based on the size, user base, functionality, or child safety risk
42 of the Digital Platform, require the designation of additional child online safety
43 or compliance personnel as may be reasonably necessary for the effective
44 implementation of this Act.

45 The name and official contact details of the designated compliance officer and
46 any additional personnel required under this subsection shall be filed with the

1 SEC and the Office and updated within the period prescribed by the
2 appropriate agency.

3
4 (c) Registry. – The SEC shall, in coordination with the Office, maintain a publicly
5 accessible registry of Digital Platforms containing such information as may be
6 necessary for identification, regulatory coordination, and public accountability,
7 subject to applicable laws on privacy and confidentiality.

8
9 (d) Updating of Information. – Digital Platforms shall notify the SEC and the
10 Office of any material change in their registered information, local
11 representative, resident agent, or designated compliance officer within the
12 period and in the manner prescribed by the appropriate agency.

13
14 (e) Compliance with Other Laws. – Registration and local presence under this
15 section shall be without prejudice to the authority of the Office, the SEC, and
16 other competent government agencies under this Act and other applicable
17 laws.

18 **SEC. 14. Compliance and Transparency Reports.** – Digital Platforms shall submit
19 to the Office periodic compliance and transparency reports in such form, frequency,
20 and manner as may be prescribed in the IRR.

21 Such reports shall, as applicable, contain information on measures adopted to
22 comply with this Act, including Age Assurance and child-safety measures, aggregated
23 or appropriately anonymized information on complaints and reports involving children,
24 actions taken in response thereto, and other information reasonably necessary and
25 proportionate to assess compliance with this Act and systemic child safety risks.

26 The Office shall prescribe reporting requirements proportionate to the size,
27 nature, reach, functionality, and level of risk of the Digital Platforms, and shall ensure
28 that such requirements do not unnecessarily require the disclosure of personal or
29 sensitive personal information or other information protected under applicable laws.

30 **SEC. 15. Community and Stakeholder Participation.** – The Office shall establish
31 mechanisms for meaningful, inclusive, and age and developmentally appropriate
32 participation and consultation with children, parents and parent-substitutes,
33 child-protection, child-development, health, digital-safety, and other relevant experts,
34 CSOs, educators, industry stakeholders, and other relevant sectors in the
35 development, implementation, monitoring, and periodic review of policies, standards,
36 and programs under this Act.

37 In developing and reviewing the measures under this Act, the Office shall
38 consider and appropriately respond to the rights, views, needs, and diverse
39 circumstances of children, particularly children in vulnerable or disadvantaged
40 situations, and shall ensure that mechanisms for participation are accessible and do
41 not expose children to undue risks to their safety, privacy, or well-being.

42 **SEC. 16. Age Assurance Framework.** – All Digital Platforms shall develop,
43 implement, maintain, and submit to the Office an Age Assurance framework, in such
44 form and manner as the Office may prescribe.

1 The framework shall describe the Age Assurance methods employed, the
2 corresponding age-based protections and access controls, and the measures adopted
3 to ensure the privacy, security, and confidentiality of users. Such framework shall
4 provide for a reasonable, proportionate, effective, and privacy-preserving system of
5 Age Assurance sufficient to determine if a user is a child and, where necessary, the
6 applicable age or age range of such user.

7 The Digital Platforms shall be responsible for the effectiveness of their
8 respective Age Assurance systems, including reverifying their user's age at least twice
9 a year, and shall not be deemed compliant solely by requiring a user to enter or declare
10 a date of birth.

11 Age Assurance measures shall collect and retain only such information as is
12 reasonably necessary for age determination and shall not be used for advertising,
13 profiling, commercial exploitation, or any purpose unrelated to safety, legal
14 compliance, account security, or Age Assurance.

15 Where the age of a user cannot reasonably be established, the more protective
16 applicable age classification shall apply until sufficient Age Assurance has been
17 completed.

18 The Office may review the Age Assurance framework and require its revision,
19 updating, or enhancement to ensure compliance with this Act and other applicable
20 laws, rules, and regulations.

21 CHAPTER IV

22 DUTIES AND RESPONSIBILITIES OF STAKEHOLDERS

23 **SEC. 17. *Parents and Parent-Substitutes.*** – Parents and parent-substitutes shall
24 promote the safe, responsible, and age-appropriate use of social media and online
25 games by children under their care, consistent with the child's best interests. They
26 shall provide appropriate guidance and supervision, give informed parental consent
27 when required under this Act, and promote online safety, responsible digital
28 citizenship, healthy digital habits, and the use of available privacy, security, and
29 child-safety measures.

30 Parents and parent-substitutes shall report to the appropriate social media
31 platform or government authority, activities that reasonably appear to expose a child
32 to abuse, exploitation, cyberbullying, online grooming, or other suspected violations of
33 this Act, and cooperate, when appropriate, with relevant institutions, government
34 agencies, and CSOs in promoting child online safety and digital literacy.

35 The failure or omission of a parent or parent-substitute to discharge any duty
36 or responsibility under this Act shall not relieve, exempt, diminish, or otherwise affect
37 the respective obligations, responsibilities, or liabilities of Digital Platforms, nor shall it
38 constitute a defense to any violation or penalty arising from the latter's failure to comply
39 with its duties and responsibilities herein.

40 For purposes of this Act, a parent-substitute shall secure a certification from the
41 appropriate office of the DSWD to be recognized as a parent-substitute.

SEC. 18. Application Distribution and Operating System Providers.—Application Distribution and Operating System Providers that facilitate access to Social Media Platforms and Online Gaming Platforms shall implement reasonable, reliable, proportionate, and privacy-preserving mechanisms for Age Assurance consistent with the Age Assurance framework established under this Act, applicable Philippine privacy laws and other relevant laws and regulations.

They shall apply Safety by Design and Safety by Default principles in the design, development, configuration, and operation of their services and systems. They shall provide appropriate safety and privacy settings by default for users identified or reasonably estimated to be children and shall take reasonable measures to prevent children from accessing applications or features that are prohibited or restricted under this Act.

They shall not make available for download, installation, or access within the Philippines any Social Media Platform and Functionally Equivalent Digital Service to a user who is determined or reasonably estimated to be below thirteen (13) years of age, in accordance with the Age Assurance requirements of this Act. Further, they shall restrict access to applications or features designated as age-restricted for users thirteen (13) years of age to below eighteen (18) years of age and shall provide mechanisms for parental consent where required under this Act.

SEC. 19. Social Media Platforms.— Social Media Platforms subject to this Act have the affirmative and continuing duty to strictly comply with the age restrictions prescribed under this Act and to apply Safety by Design, Safety by Default, and age-appropriate design principles throughout the design, development, configuration, deployment, operation, moderation and continuous improvement of their services, taking into account the age, developmental capacity, and best interests of the child.

For this purpose, Social Media Platforms shall:

- (a) Establish age or age ranges, taking into account internationally recognized standards on child development and online safety, and ensure that content, features, advertisements, recommendations, communications, and functionalities made available to children are appropriate to their age or applicable age range and compliant with the provisions of this Act;
- (b) Apply, by default and upon determining or reasonably estimating that a user is a child, the highest level of privacy and safety protection appropriate to the child's age or applicable age range and the risks involved;
- (c) Exclude content, advertisements, recommendations, features, and interactions that are harmful, prohibited, or inappropriate to the child's age or developmental capacity;
- (d) Prohibit minors from direct communications and interactions, particularly with unknown adults, and unless expressly allowed by the Office and subject to appropriate safeguards, prohibit interactions with Artificial Intelligence Systems, including AI chatbots, virtual assistants, and other AI-enabled features, to prevent exposure to harmful, inappropriate, manipulative, or exploitative interactions, taking into account the child's age and developmental capacity;

- (e) Disable by default public visibility, precise geolocation, targeted advertising, behavioral profiling, unnecessary collection or sharing of personal information, and other practices that may expose children to undue risks;
- (f) Permanently disable the monetization, paid promotion, or algorithmic amplification for commercial gain of content that exploits a child's distress, humiliation, punishment, injury, abuse, medical emergency, displacement, grief, or other circumstances in a manner inconsistent with the child's dignity, privacy, safety, or best interests;
- (g) Design and operate appropriate processes to identify, prevent, and mitigate reasonably foreseeable and material risks to children, including exposure to Harmful or Prohibited Content, Livestreaming, exploitation, and patterns of use that may adversely affect their safety, health, development, education, sleep, or well-being;
- (h) Prohibit minors from publishing through Livestreaming and other similar features, as well as the use of endless scrolling, autoplay, short-form video feeds or "shorts," intrusive notifications, and other features reasonably likely to encourage prolonged, repetitive, or difficult-to-control use, and apply age-appropriate time limits and safeguards to such features;
- (i) Disable purchases, gambling-like mechanisms, and other age-restricted transactions unless permitted under applicable law and subject to appropriate safeguards;
- (j) Conduct and periodically update documented Child Safety Risk Assessments that identifies and evaluates reasonably foreseeable and material risks to the rights, safety, health, privacy, development, and well-being of children arising from the service's design, operation, features, algorithms, Recommender Systems, Artificial Intelligence Systems, including risks of exposure to, or radicalization toward, violent extremism, and other relevant functionalities, and implement measures to prevent, mitigate, and address identified risks;
- (k) Where Parental Consent is specifically required under this Act or other applicable laws for a particular transaction, purchase, disclosure, collection or processing of information, or other activity, obtain reasonable assurance that the person giving such consent is an adult and is the child's parent or parent-substitute: *Provided*, That a mere declaration, checkbox, entry of a date of birth, possession of the child's account credentials, or similar form of self-certification shall not, by itself, constitute sufficient assurance of such authority: *Provided, further*, That verification shall be proportionate to the nature and risk of the activity and shall collect and retain no more personal information than is reasonably necessary, in accordance with applicable Philippine privacy laws and other relevant laws and regulations;
- (l) Provide accessible, child-friendly, and effective reporting, complaint, appeal, parental supervision, and redress mechanisms, together with clear and age-appropriate information on safety and privacy controls;
- (m) Maintain appropriate and meaningful human oversight of automated systems and promptly address harmful content, unsafe interactions, prohibited accounts, and violations of this Act; and
- (n) Implement such other safeguards as may be necessary to address reasonably foreseeable and material risks to the safety, privacy, development, and well-being of children, as may be prescribed by the Office.

1 Social Media Platforms and Functionally Equivalent Digital Services shall be
2 accountable for reasonably foreseeable risks arising from the design, operation,
3 features, algorithms, and other functionalities of their services and for failure to
4 implement the safeguards required under this Act.

5 **SEC. 20. Online Gaming Platforms.** – With respect to their social, communication,
6 content-sharing, Livestreaming, user-interaction, recommender, or other interactive
7 features and functionalities, Online Gaming Platforms shall:

- 8 (a) Strictly comply with the age restrictions prescribed under this Act and
9 apply Safety by Design, Safety by Default, and age-appropriate design
10 principles;
- 11 (b) Implement appropriate Age Assurance framework and automatically
12 apply appropriate privacy and safety protections to users determined or
13 reasonably estimated to be children. Where age cannot be reasonably
14 established, the more protective age classification shall apply until
15 verified;
- 16 (c) Prevent and prohibit Harmful or Prohibited Content communicated
17 through text, voice, images, videos, or other interactive features or
18 functionalities of the platform, including its creation, posting, accessing,
19 consumption, sharing, transmission, or dissemination;
- 20 (d) Prohibit direct communications and interactions with other users and
21 AI Systems;
- 22 (e) Prohibit Livestreaming, endless scrolling, and short-form video feeds or
23 “shorts,” where such features are available and accessible to users, and
24 apply age-appropriate limits and safeguards to other features reasonably
25 likely to encourage prolonged, repetitive, or difficult-to-control use,
26 including intrusive notifications, and similar features;
- 27 (f) Disable targeted advertising, behavioral profiling, unnecessary collection
28 or sharing of information, purchases, gambling-like mechanisms, and
29 other age-restricted activities accessible through the platform;
- 30 (g) Conduct and periodically update a Child Safety Risk Assessment and
31 implement measures to prevent, mitigate, and address identified risks;
- 32 (h) Provide accessible, child-friendly, and effective reporting, complaint,
33 appeal, parental supervision, and redress mechanisms;
- 34 (i) Maintain appropriate human oversight of automated systems used in the
35 features and functionalities and promptly address harmful content,
36 unsafe interactions, prohibited accounts, and violations of this Act; and
- 37 (j) Implement such other safeguards as may be necessary to address
38 reasonably foreseeable and material risks to the safety, privacy,
39 development, and well-being of children arising from the features and
40 functionalities, as may be prescribed by the Office.

1 Nothing in this section shall be construed to regulate the core gameplay, game
2 mechanics, or other functions of an Online Gaming Platform that do not involve the
3 features and functionalities prohibited in this Act.

4 **SEC. 21. Accountability of Digital Platforms.** – The respective duties and
5 responsibilities under Chapter IV of this Act shall remain with the Digital Platforms,
6 and shall not be transferred to, or made dependent upon, the child or the child's parent
7 or parent-substitute taking affirmative steps to secure the child's protection. Parental
8 consent, supervision, or use of safety tools shall not relieve the Digital Platforms of
9 their respective duties, responsibilities, or accountability under this Act. Neither shall
10 a Digital Platform avoid or diminish its duties, responsibilities, or liability under this Act
11 on the following grounds:

- 12 (a) A child misrepresented the child's age, failed to activate available safety or
13 privacy settings, or failed to obtain parental consent;
- 14 (b) A person falsely represented oneself to be the child's parent, guardian, or
15 other legally authorized representative; or
- 16 (c) Its terms of service prohibit access by children below a specified age, where
17 the Digital Platform knew or reasonably should have known that its service
18 was being accessed or used by children, or failed to take the measures
19 required under this Act to enforce applicable age restrictions and safeguards.

20 **SEC. 22. Internet Service Providers.** – Internet Service Providers shall:

- 21 (a) Cooperate with the DICT, through the Office, the NTC, law enforcement
22 agencies, and other competent government authorities in the implementation
23 of this Act;
24
- 25 (b) Comply with lawful orders, warrants, preservation requests, and other lawful
26 directives issued by competent government authorities in accordance with
27 applicable laws and due process;
28
- 29 (c) Preserve relevant traffic, subscriber, and other data in their possession or
30 control when lawfully required by a competent government authority, subject
31 to applicable data privacy, confidentiality, and data retention laws;
32
- 33 (d) Establish and maintain accessible channels for receiving and responding to
34 lawful requests and notices concerning child online safety and suspected
35 violations of this Act;
36
- 37 (e) Take reasonable measures to facilitate the implementation of lawful blocking,
38 restriction, or other access measures ordered by a competent government
39 authority under this Act or other applicable laws; and
40
- 41 (f) Provide information and assistance reasonably necessary for the investigation
42 of suspected violations of this Act when lawfully required, subject to applicable
43 laws on privacy, confidentiality, due process, and freedom of expression.

44 **CHAPTER V**

45 **DATA PRIVACY AND CONFIDENTIALITY**

46 **SEC. 23. Privacy and Confidentiality.** – All personal information, records, reports,
47 and other information obtained, collected, processed, stored, disclosed, or otherwise

maintained pursuant to this Act shall be protected and processed in accordance with applicable Philippine privacy laws and other relevant laws and regulations.

Such information shall not be disclosed except as authorized by law or when necessary and lawful for the implementation or enforcement of this Act, subject to appropriate safeguards, applicable confidentiality requirements, and the principles of necessity and proportionality.

Nothing in this Act shall be construed as authorizing the collection, processing, retention, or disclosure of personal information beyond what is necessary and lawful for the purposes of this Act.

SEC. 24. Data Processing Principles. – Without prejudice to applicable Philippine privacy laws and other relevant laws and regulations, the Digital Platforms, the DICT, and all persons, entities, and government agencies processing personal information pursuant to this Act shall process personal information only on a lawful basis and in accordance with the principles of transparency, legitimate purpose, and proportionality.

Personal information processed pursuant to this Act shall be, as applicable:

- (a) Collected for specified, explicit, and legitimate purposes and processed only in a manner compatible with such purposes;
- (b) Processed fairly and lawfully;
- (c) Adequate, relevant, necessary, and not excessive in relation to the purposes for which it is processed;
- (d) Accurate and, where necessary, kept up to date;
- (e) Retained only for as long as necessary to fulfill the lawful purposes for which it was collected or as otherwise authorized or required by law; and
- (f) Protected through reasonable and appropriate organizational, physical, and technical measures against unauthorized or unlawful processing and against accidental or unlawful loss, destruction, alteration, disclosure, or access.

Age Assurance under this Act shall, to the extent reasonably practicable, be implemented through privacy-preserving mechanisms that minimize the collection, retention, use, and disclosure of children's personal information and age-related information. Age Assurance may be facilitated through the verification of a person's age using the Philippine Identification System (PhilSys) or other government-administered identity verification systems, including e-Verify or its equivalent, through the appropriate government agency or duly authorized government entity, without requiring the Digital Platforms subject to this Act to collect, retain, or access the individual's government-issued identification document or more personal information than is necessary for the purpose of Age Assurance.

Nothing in this Act shall deny or restrict any person's lawful access to Social Media Platforms and Online Gaming Platforms solely by reason of the absence of a record pertaining to such person in the PhilSys. The IRR shall provide for alternative, privacy-preserving Age Assurance mechanisms for persons without a PhilSys record, consistent with this Act, applicable Philippine privacy laws, and other relevant laws and regulations.

CHAPTER VI

COMPLIANCE AND ADMINISTRATIVE PROCEEDINGS

SEC. 25. Compliance Monitoring and Preliminary Investigation. – The Office may, *motu proprio* or upon receipt of a complaint or other sufficient information, conduct compliance monitoring, inspection, audit, technical assessment, or preliminary investigation where there are reasonable grounds to believe that a Social Media Platform, Online Gaming Platform, or App Distribution and Operating System Provider has violated or failed to comply with this Act, its IRR, or any lawful order or issuance issued pursuant thereto.

For this purpose, the Office may require the submission of relevant information, records, reports, policies, and other documents reasonably necessary to determine compliance, subject to applicable laws on privacy, confidentiality, due process, and data protection.

SEC. 26. Notice of Violation and Corrective Measures. – Where the Office finds reasonable grounds to believe that a violation of this Act has been committed, it shall issue a written notice of violation stating the nature of the alleged violation, the factual basis thereof, and the applicable provisions of law, rules, or regulations allegedly violated.

The respondent Digital Platform shall be afforded due notice and a reasonable opportunity to submit an explanation, present evidence, or otherwise respond to the allegations within the prescribed period.

Where appropriate, the Office may allow or require the respondent Digital Platform to undertake corrective measures or submit a compliance plan within a prescribed period, taking into consideration the nature and gravity of the alleged violation, the risks posed to children, the respondent's good faith and cooperation, and the need for prompt compliance. Such corrective measures or compliance plan shall be regulatory and remedial in nature and shall not constitute a determination of administrative liability or the imposition of an administrative sanction.

Where the alleged violation is not satisfactorily addressed within the prescribed period, the Office shall refer the matter, together with its findings, investigation report, and supporting records and evidence, to the NTC for administrative adjudication in accordance with this Act.

SEC. 27. Immediate Protective and Corrective Measures. – Where the Office determines, based on reasonable grounds, that a Digital Platform's act, omission, feature, practice, or activity presents an imminent and substantial risk to the safety or well-being of children, the Office may, pending the completion of compliance proceedings and without prejudice to the jurisdiction of the NTC, direct such Digital Platform to implement such immediate and proportionate protective or corrective measures, including the preservation of relevant documents, records, computer data, electronic communications, logs, metadata, and other evidence, as may be necessary to address the identified risk, including the temporary restriction, suspension, or modification of a specific feature, function, practice, or activity.

1 Any order issued under this section shall be in writing and shall state the factual
2 and legal basis for the measure, the specific risk identified, the measure required, and
3 its scope and duration. Any such measure shall remain in effect only for the period
4 reasonably necessary to address the identified risk and shall be subject to prompt
5 review or reconsideration upon the request of the affected party, without prejudice to
6 the administrative adjudicatory jurisdiction of the NTC.

7 The issuance or implementation of a measure under this section shall not
8 constitute a finding of administrative liability or the imposition of an administrative
9 penalty, which shall remain within the jurisdiction of the NTC under this Act.

10 **SEC. 28. Administrative Proceedings and Adjudication.** – Upon referral by the
11 Office following compliance monitoring or preliminary investigation, or upon the filing
12 of an administrative complaint involving a violation subject to administrative sanctions
13 under this Act, the NTC shall conduct the appropriate administrative proceedings in
14 accordance with due process and its applicable rules of procedure.

15 The NTC shall afford the respondent due notice and a reasonable opportunity
16 to be heard, require the submission of documents and other evidence, and issue
17 subpoenas and subpoenas duces tecum in accordance with law. The NTC shall
18 determine administrative liability based on substantial evidence and, where warranted,
19 impose the administrative penalties provided under this Act.

20 The NTC may consider the findings, records, and evidence gathered by the
21 Office in the course of its compliance monitoring or preliminary investigation, without
22 prejudice to the NTC's independent determination of administrative liability.

23 **SEC. 29. Administrative Remedies and Appeal.** – A party aggrieved by a decision
24 or order of the NTC may file a motion for reconsideration within fifteen (15) days from
25 receipt thereof, in accordance with the applicable rules of procedure.

26 A final decision or order of the NTC may be appealed or reviewed in accordance
27 with applicable laws and rules of procedure.

28 The filing of a motion for reconsideration or appeal shall not automatically stay
29 the execution of the assailed decision or order, unless otherwise provided by law or a
30 stay is granted by the appropriate authority pursuant to applicable law and rules of
31 procedure.

32 **SEC. 30. Referral to Appropriate Authorities and Handling of Related**
33 **Evidence.** – Where information reasonably indicates the commission of a criminal
34 offense, the Office shall promptly refer the matter to the appropriate law enforcement or
35 prosecution authority. For offenses involving information and communications
36 technology, computer systems, online platforms, electronic communications, or other
37 cybercrime-related matters, the Cybercrime Investigation and Coordinating Center
38 (CICC) shall be included for coordination and monitoring, consistent with R.A. No. 10175.
39

40 Upon discovery of information indicating the commission of a criminal offense, the
41 Office or other concerned entity shall take appropriate and lawful measures to secure
42 and preserve relevant documents, records, computer data, electronic communications,
43 logs, metadata, and other evidence, in accordance with R.A. No. 10175, R.A. No. 10173,
44 the Rules on Electronic Evidence, and other applicable laws and rules.

For cybercrime-related matters, the CICC may facilitate coordination with the Philippine National Police (PNP), the National Bureau of Investigation (NBI), the Department of Justice-Office of Cybercrime (DOJ-OOC), and other competent authorities to ensure the timely initiation of lawful evidence-preservation procedures.

CHAPTER VII

ADMINISTRATIVE OFFENSES AND PENALTIES

SEC. 31. *Administrative Liability.* – The Digital Platforms shall be administratively liable for failure to perform their duties and responsibilities under this Act, its IRR, and other applicable laws, and any violation thereof, in accordance with the applicable rules of procedure.

SEC. 32. *Administrative Penalties.* – Upon a determination of administrative liability, the NTC may impose the following fines, without prejudice to other administrative measures expressly authorized under this Act:

(a) Violations of Procedural and Compliance Requirements. – Digital Platforms that fail to comply with registration, designation of a compliance officer, reporting, record-keeping, notification, or other procedural and compliance requirements expressly imposed under this Act shall be subject to:

(1) First violation – a fine of not less than One hundred thousand pesos (₱100,000.00) but not more than Five hundred thousand pesos (₱500,000.00);

(2) Second violation – a fine of not less than Five hundred thousand pesos (₱500,000.00) but not more than One million pesos (₱1,000,000.00); and

(3) Third and each subsequent violation – a fine of not less than One million pesos (₱1,000,000.00) but not more than Two million pesos (₱2,000,000.00).

(b) Violations of Child-Safety Obligations. – Digital Platforms that fail to comply with a child-safety obligation expressly imposed under this Act, including obligations relating to Age Assurance, child account safeguards, safety by design and safety by default measures, protection against specified online risks, or other child-safety obligations expressly imposed under this Act, shall be subject to:

(1) First violation – a fine of not less than Two million pesos (₱2,000,000.00) but not more than Five million pesos (₱5,000,000.00);

(2) Second violation – a fine of not less than Five million pesos (₱5,000,000.00) but not more than Ten million pesos (₱10,000,000.00); and

(3) Third and each subsequent violation – a fine of not less than Ten million pesos (₱10,000,000.00) but not more than Twenty million pesos (₱20,000,000.00).

SEC. 33. Continuing Violations. – Where a violation consists of a continuing failure to comply with an obligation or a final and executory order under this Act, the NTC may impose a daily fine after the period prescribed for compliance has lapsed, subject to due notice and reasonable opportunity to comply.

The daily fine shall not be less than One hundred thousand pesos (₱100,000.00) nor more than One million pesos (₱1,000,000.00) per day, as determined by the NTC in accordance with the factors under Section 33 of this Act.

The imposition of a daily fine shall cease upon actual compliance, as determined by the NTC on the basis of substantial evidence.

SEC. 34. Disposition of Administrative Fines. – Administrative fines collected under this Act shall accrue to the National Treasury and shall be accounted for and disbursed in accordance with existing budgeting, accounting, and auditing laws, rules, and regulations.

SEC. 35. Restriction and Prohibition of Operation. – In addition to the fines, Digital Platform found noncompliant with the duties and responsibilities under this Act, despite prior notice and opportunity to comply, may, after due process, be subject to temporary restriction of access within the Philippines until full compliance is achieved, or, in cases of repeated and serious violations, be prohibited from operating in the Philippines.

SEC. 36. Civil and Criminal Liability. – The imposition of administrative liability or penalties under this Act shall be without prejudice to the institution of appropriate civil, criminal, or other administrative proceedings under this Act or other applicable laws.

CHAPTER VIII

SUPPORTIVE AND EDUCATIONAL MEASURES

SEC. 37. Educational and Community-Based Measures for Parents and Parent-Substitutes. – Consistent with the policy of promoting responsible digital parenting and strengthening the capacity of parents and parent-substitutes to protect children in the digital environment, the DICT, in coordination with the DSWD, DepEd, local government units, and other appropriate agencies, may provide educational, supportive, and community-based measures for parents and parent-substitutes who may benefit from assistance in fulfilling their responsibilities under this Act.

Such measures may include digital literacy, online safety, responsible digital parenting, parental guidance and supervision, child online protection, and other appropriate educational, supportive, or community-based programs designed to enhance the knowledge, skills, and capacity of parents and parent-substitutes to guide and protect children in the digital environment.

The measures under this section shall be educational, supportive, and capacity-building in nature, proportionate to the circumstances, and implemented in a manner consistent with the best interests of the child, the rights and responsibilities of parents and parent-substitutes, the child's evolving capacities, and applicable privacy and due process protections.

1 Nothing in this section shall be construed to impose administrative liability or a
2 monetary penalty upon a parent or parent-substitute solely by reason of a child's
3 access to Digital Platforms or use of a prohibited feature or functionality.

4 CHAPTER IX

5 FINAL PROVISIONS

6 **SEC. 38. Congressional Oversight Committee.** – There is hereby created a
7 Congressional Oversight Committee (COC) to monitor and oversee the
8 implementation of the provisions of this Act. The COC shall be composed of five (5)
9 members of the House of Representatives and five (5) members of the Senate. The
10 minority shall be entitled to pro rata representation but shall have at least one (1)
11 representative from each Chamber. It shall be jointly chaired by the Committee on
12 Welfare of Children Chairperson for the House of Representatives and the Committee
13 on Women, Children, Family Relations and Gender Equality Chairperson for the
14 Senate.

15 **SEC. 39. Annual Report on Child Online Safety.** – The DICT and the NTC shall,
16 not later than March 31 of every year, submit to the President and the Congress of the
17 Philippines an annual report on the implementation of this Act, including:

- 18 (a) Status of compliance and enforcement;
- 19 (b) Regulatory, compliance, monitoring, and preliminary investigative activities
20 undertaken by the DICT and the Office, and adjudicatory activities
21 undertaken by the NTC;
- 22 (c) Emerging child online safety risks and developments; and
- 23 (d) Recommendations to strengthen child online safety.

24 The report shall comply with applicable laws on data privacy, confidentiality,
25 privilege, and disclosure, and shall not compromise pending proceedings. The DICT
26 and NTC shall make available to the public an executive summary of the report,
27 subject to applicable laws.

28 **SEC. 40. Appropriations.** – The amount necessary for the initial implementation of
29 this Act shall be charged against the current year's appropriations of the DICT.
30 Thereafter, the amount needed for the continued implementation of this Act shall be
31 included in the annual General Appropriations Act.

32 **SEC. 41. Implementing Rules and Regulations.** – Within ninety (90) days from the
33 effectivity of this Act, the Secretary of Information and Communications Technology
34 shall, through the Office, and the NTC, within their respective mandates and in
35 consultation with the CICC, DOJ, NPC, PSA, CWC, and other concerned government
36 agencies, CSOs, and other stakeholders, promulgate the necessary IRR for the
37 effective administration and enforcement of this Act.

38 **SEC. 42. Transitory Provision.** – Within one hundred twenty (120) days from the
39 effectivity of this Act, the DICT shall, in coordination with the NTC and other concerned
40 government agencies, undertake the necessary organizational, regulatory, technical,
41 and administrative measures for its implementation, within their respective mandates.

1 Pending the full operationalization of the mechanisms required under this Act,
2 the DICT and NTC shall perform their respective functions using their existing
3 organizational structures, personnel, systems, and resources, insofar as consistent
4 with this Act.

5 Existing policies, programs, systems, agreements, and mechanisms relating to
6 the protection of children in the digital environment shall continue to operate, insofar
7 as consistent with this Act, until amended, repealed, or superseded.

8 **SEC. 43. Separability Clause.** – If any provision or part of this Act is declared
9 unconstitutional or invalid, the remaining parts or provisions not affected shall remain
10 in force and effect.

11 **SEC. 44. Repealing Clause.** – All laws, decrees, orders, and rules and regulations,
12 contrary to or inconsistent with the provisions of this Act are amended or repealed
13 accordingly.

14 **SEC. 45. Effectivity.** – This Act shall take effect fifteen (15) days after its publication
15 in the *Official Gazette* or in a newspaper of general circulation.

Approved,