

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
Second Regular Session
House Bill No. **11265**



Introduced by: Congressman **BIENVENIDO M. ABANTE, JR.**

AN ACT
PROHIBITING CHILDREN BELOW TWELVE (12) YEARS OF AGE FROM
CREATING OR MAINTAINING PERSONAL SOCIAL-MEDIA ACCOUNTS,
PROVIDING FOR CHILD-SAFETY MECHANISMS, PLATFORM
ACCOUNTABILITY, AND FOR OTHER PURPOSES

EXPLANATORY NOTE

“Lo, children are an heritage of the LORD: and the fruit of the womb is his reward.”
— *Psalms 127:3 (KJV)*

“The State shall defend the right of children to assistance, including proper care and nutrition, and special protection from all forms of neglect, abuse, cruelty, exploitation and other conditions prejudicial to their development.” — *Article XV, Section 3(2), 1987 Constitution*

The Holy Writ warns of a generation that “curseth their father,” is “pure in their own eyes,” has “lofty” eyes, and whose words are like “swords” and “knives” that harm the poor and needy (*Proverbs 30:11-14, KJV*). In today’s digital age, social media can amplify and normalize the disrespect, self-righteousness, pride, cruelty, and harmful behavior described in these passages. Young children, whose judgment and character are still developing, are particularly vulnerable to absorbing, imitating, or becoming victims of such influences. The State must therefore establish reasonable safeguards to protect them from premature exposure to online environment they may not yet be equipped to navigate safely and responsibly.

Against this moral and constitutional backdrop, children increasingly encounter digital technologies at home and through social-media services. While digital technologies may provide communication and access to information, social-media platforms may also expose young children to grooming, luring, online sexual abuse or exploitation, cyberbullying, harmful content, privacy violations, fraudulent schemes, excessive screen use, and manipulative design.

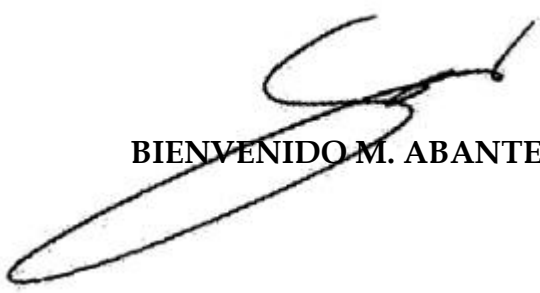
Young children below twelve (12) years of age require heightened protection because of their developing capacity to assess risks, understand privacy consequences, identify manipulation, and protect themselves from online abuse and exploitation.

This bill therefore prohibits children below twelve (12) years of age from creating, registering, operating, or maintaining personal social-media accounts, but does not prohibit them from accessing the internet generally, viewing publicly available lawful content, or using an account controlled by a parent, guardian, government agency, or institution for a lawful non-personal purpose.

Under the bill, covered platforms are mandated to take reasonable and proportionate measures to prevent children below twelve (12) years of age from creating or maintaining personal social-media accounts. They shall apply child-safety safeguards, provide child-friendly reporting mechanisms, restrict unlawful and seriously harmful content, and refrain from using age-assurance information for targeted advertising or behavioral profiling.

The bill likewise requires privacy-preserving age assurance and prohibits the routine collection of government-issued identification documents and biometric information. It also requires covered platforms to maintain child-safety programs, designate responsible officers, establish reporting and appeals mechanisms, and cooperate with competent government authorities.

In view of the foregoing, the immediate approval of this measure is earnestly sought.



BIENVENIDO M. ABANTE, JR.

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
Second Regular Session
House Bill No. **11265**

Introduced by: Congressman **BIENVENIDO M. ABANTE, JR.**

AN ACT
PROHIBITING CHILDREN BELOW TWELVE (12) YEARS OF AGE FROM
CREATING OR MAINTAINING PERSONAL SOCIAL-MEDIA ACCOUNTS,
PROVIDING FOR CHILD-SAFETY MECHANISMS, PLATFORM
ACCOUNTABILITY, AND FOR OTHER PURPOSES

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

SECTION 1. *Short Title.* — This Act shall be known as the “Child Online Safety and Social Media Accountability Act.”

SEC. 2. *Declaration of Policy.* — It is the policy of the State to protect children from abuse, exploitation, violence, harassment, grooming, luring, cyberbullying, trafficking, privacy violations, fraudulent schemes, manipulative design, harmful content, and excessive or compulsive use arising from social-media services and other digital technologies.

The State recognizes that digital technologies may provide access to information, communication, creativity, and participation. Regulation under this Act shall be age-appropriate, proportionate, privacy-protective, and consistent with the best interests and evolving capacities of children.

SEC. 3. *Definition of Terms.* — For purposes of this Act:

- (a) *Child* refers to a person below eighteen (18) years of age.
- (b) *Age assurance* refers to a reasonable process of determining or estimating whether a user belongs to a specified age group. It may include age declaration, age estimation, age verification, parental attestation, or a combination thereof.
- (c) *Personal social-media account* refers to an account, profile, channel, or page controlled by an individual user that enables the user to interact with other users or to create, upload, share, view, recommend, comment on, livestream, or otherwise engage with user-generated content.

The term excludes an account or page established and controlled by a parent, guardian, government agency, or institution when used solely for a lawful non-personal purpose and not as the child's personal account.

- (d) *Social-media platform* refers to an internet-based service, application, or website whose primary purpose is to enable users to view, create, share, recommend, comment on, livestream, or otherwise interact with user-generated content or other users.

The term includes social-networking, video-sharing, livestreaming, blogging, picture-sharing, file-sharing, and similar services.

The term does not include:

- (1) private electronic communications used exclusively between identified persons;
- (2) services primarily designed and used for health care, government services, emergency assistance, or public-service information; or
- (3) professional-communication services in which social interaction is merely incidental to the principal professional purpose.

The implementing rules and regulations may prescribe objective criteria for determining whether a service is covered, taking into account its principal purpose, audience, functionality, and risk to children.

- (e) *Platform* refers to a social-media platform covered by this Act.
- (f) *Responsible officer* refers to the officer designated by a covered platform who has actual authority over the platform's child-safety and compliance functions.
- (g) *Unknown adult* refers to an adult user who is not an approved contact, known family member, verified caregiver, or other person authorized by the child's parent or guardian or by applicable law.
- (h) *Large or high-risk platform* refers to a platform that meets the user-volume, functionality, revenue, audience, or child-risk thresholds prescribed in the implementing rules and regulations of this Act.
- (i) *Dark pattern or deceptive design pattern* refers to a user-interface or user-experience design, practice, or feature that materially subverts, impairs, or distorts a user's autonomy, decision-making, or ability to give informed consent, including through concealment, confusing language, preselected

options, excessive information, emotional manipulation, or unequal presentation of choices.

- (j) *Zero-knowledge proof or ZKP* refers to a cryptographic method by which a user proves that the user satisfies a specified age requirement without disclosing the user's identity, date of birth, or other unnecessary personal information.
- (k) *Third-party tokenization* refers to the issuance by an independent and qualified service provider of a cryptographic or equivalent token confirming that a user has satisfied an age requirement, without disclosing the underlying identity or personal information to the platform, except when required by law.
- (l) *Native child profile* refers to a child-safety or family-management profile maintained by a device operating system, browser, application store, or comparable technical service, which may communicate a privacy-preserving age-group or parental-control status to a platform.
- (m) *Geo-blocking* refers to a technical measure that restricts access to specified digital content, functions, services, domains, or websites from a particular jurisdiction.

SEC. 4. *Public Content and Child-Safety Safeguards.* — A platform that permits children below twelve (12) years of age to view public content shall:

- (a) apply the highest available child-safety and privacy settings by default, where technically practicable;
- (b) use reasonable age-appropriate filtering, content warnings, and access controls for:
 - (1) unlawful content;
 - (2) sexually explicit content harmful to children;
 - (3) content that promotes or facilitates child exploitation, trafficking, grooming, or luring;
 - (4) content that depicts or promotes extreme violence or self-harm and presents a serious and identifiable risk of harm to children; and
 - (5) other content categories identified in the implementing rules and regulations after public consultation;
- (c) prevent the recommendation or targeted promotion to children of unlawful content or content presenting a serious risk of harm;

- (d) provide a prominent, child-friendly reporting mechanism; and
- (e) promptly restrict, remove, or refer specifically identified unlawful content in accordance with applicable laws.

Any restriction on public content shall be specific, necessary, proportionate, and subject to correction and appeal.

SEC. 5. *Safeguards for Child Access to Public Content.* — A covered platform shall, where technically practicable:

- (a) restrict unsolicited direct messages, invitations, and other communications from unknown adults to children;
- (b) disable location-sharing by default for child-accessible profiles or interfaces;
- (c) prohibit targeted advertising and behavioral profiling based on information concerning a child;
- (d) disable personalized recommendations based on a child's personal information or activity, except when strictly necessary for safety, security, or accessibility and permitted by law; and
- (e) provide clear, age-appropriate, and accessible explanations of its safety tools, reporting procedures, and content restrictions.

SEC. 6. *Privacy-Preserving Age Assurance.* — A platform shall use age-assurance measures reasonably appropriate to the risks, size, audience, and features of its service.

Age assurance shall:

- (a) collect and retain only information reasonably necessary for age determination, child safety, or legal compliance;
- (b) use the least intrusive effective method reasonably available;
- (c) not routinely require or retain copies of government-issued identification documents;
- (d) not require biometric information unless expressly authorized by law and shown to be necessary and proportionate to a specific child-protection risk;
- (e) not use age-assurance information for targeted advertising, behavioral profiling, or any purpose unrelated to child safety or legal compliance;

- (f) protect against the public disclosure of a child's identity, age, school, residence, or family relationship;
- (g) provide a reasonable and timely procedure to correct an erroneous age determination; and
- (h) delete age-assurance information when no longer necessary, unless retention is required by law or necessary for a specific, documented investigation or prosecution.

The National Privacy Commission shall issue privacy and security standards for the collection, processing, access, retention, deletion, breach response, and independent audit of age-assurance information.

SEC. 7. *Authorized Age-Assurance Methodologies.* —

- (a) An age-assurance token shall disclose to the platform only the minimum information necessary to establish if the user is below twelve (12) years of age. It shall not disclose the user's name, exact date of birth, government identification number, address, school, biometric information, or other identifying information unless required by law.
- (b) A large or high-risk platform shall bear the cost of any age-assurance mechanism that it requires or designates. No child, parent, guardian, school, or low-income user shall be charged a fee solely to comply with this Act.
- (c) No platform shall require a single age-assurance methodology where another reasonably available methodology would provide equivalent protection with less collection or processing of personal information.

SEC. 8. *Child Online Safety Program.* — A covered platform shall establish and maintain a documented Child Online Safety Program proportionate to the nature, size, audience, and risks of its service.

The Program shall include:

- (a) risk assessment and mitigation procedures;
- (b) safeguards against personal social-media accounts being created or maintained by children below twelve (12) years of age;
- (c) accessible child-safety tools and reporting mechanisms;
- (d) measures against unsolicited contact between children and unknown adults;

- (e) procedures for reporting, reviewing, restricting, removing, referring, and preserving evidence relating to online sexual abuse or exploitation of children, child sexual abuse or exploitation materials, grooming, luring, trafficking, cyberbullying, threats of violence, self-harm, and other serious risks to children;
- (f) safeguards against deceptive designs, dark patterns, manipulative features, unauthorized purchases, and features designed to induce excessive or compulsive use;
- (g) designation of a responsible officer with actual authority over child-safety compliance;
- (h) an accessible and multilingual complaints and appeals system; and
- (i) submission of compliance information lawfully required by the Department of Information and Communications Technology or the National Privacy Commission, subject to confidentiality, due process, and data-protection laws.

Nothing in this Section shall require general monitoring of users or private communications.

SEC. 9. *Philippine Representative and Local Contact.* — A covered foreign platform that operates in, offers services to, or targets users in the Philippines shall designate a Philippine representative responsible for regulatory coordination, receipt of notices, complaints, and lawful requests from competent Philippine authorities.

The platform shall provide the Department of Information and Communications Technology and the National Privacy Commission with:

- (a) the name and contact details of its Philippine representative;
- (b) a physical address in the Philippines where official notices may be served; and
- (c) a dedicated electronic communication channel for child-safety, data-protection, and law-enforcement concerns.

A large or high-risk foreign platform shall maintain a physical office in the Philippines and designate a responsible officer with authority to coordinate with Philippine authorities and implement this Act, as prescribed in the implementing rules and regulations of this Act.

SEC. 10. *Prohibition on Personal Social-Media Accounts of Children Below Twelve (12) Years of Age.*

(a) It is hereby declared unlawful and punishable under this Act for a -

- (1) Child below twelve (12) years of age to create, register, operate, or maintain a personal social-media account. Likewise, it is unlawful for a parent, guardian or school to create, register, operate, or maintain, or to allow the creation, registration, operation or maintainance of a personal social-media account for such child.
- (2) Covered platform to knowingly permit a child below twelve (12) years of age to create, register, operate, or maintain a personal social-media account.

(b) The prohibition under this Section shall not be construed to prohibit a child below twelve (12) years of age from:

- (1) Accessing the internet generally;
- (2) Viewing publicly available lawful content without creating a personal social-media account;
- (3) Accessing health care, emergency assistance, government services, public-service information, or other lawful services;
- (4) Using an account controlled by a parent, guardian, government agency, or institution for a lawful non-personal purpose; or
- (5) Engaging in lawful speech, association, or other activity protected by the Constitution, provided that the activity does not involve the creation, operation or maintenance of a personal social-media account prohibited under this Act.

The foregoing shall not be used to evade the prohibition under this Section.

Nothing in this Section shall require a platform to monitor all users or private communications, but it shall take reasonable and proportionate measures to implement this Section, taking into account the risks, functionality, audience, and resources of the platform.

SEC. 11. *Prohibited Acts of Platforms.* — A platform shall not:

- (a) knowingly permit a child below twelve (12) years of age to create, register, operate, or maintain a personal social-media account;
- (b) circumvent this Act through guest mode or a substantially equivalent interactive function that enables a child below twelve (12) years of age to create or maintain a personal social-media presence;

- (c) collect or retain unnecessary information for age assurance;
- (d) use age-assurance information for advertising or behavioral profiling; or
- (e) require government identification or biometric information unless expressly authorized by law and necessary and proportionate to a specific child-protection risk.

SEC. 12. *Reporting, Restriction, and Appeals.* — A platform may temporarily restrict an account, communication, or content when reasonably necessary to prevent imminent serious harm to a child, comply with a lawful order, or preserve evidence of a suspected offense.

Except when notice would endanger a child, compromise an investigation, or facilitate an offense, the platform shall notify the affected user in clear language of the basis and duration of the action and shall provide a child-friendly appeals process and age-assurance review procedure.

SEC. 13. *Unified Reporting and Referral System.* — The Department of Information and Communications Technology, in coordination with the Department of Social Welfare and Development, Department of Education, National Privacy Commission, Department of Justice, Philippine National Police, National Bureau of Investigation, and National Coordination Center against Anti-Online Sexual Abuse or Exploitation of Children, (OSAEC) and Child Sexual Abuse or Exploitation Materials (CSAEM), shall establish or designate a unified, child-friendly reporting and referral system.

The system shall provide an online reporting portal and, where practicable, a toll-free hotline; immediate escalation of imminent danger; prompt referral of reports involving online sexual abuse or exploitation of children and child sexual abuse or exploitation materials; confidentiality and secure handling; case tracking without unnecessary disclosure of the child's identity; and protection against retaliation.

The National Coordination Center against OSAEC and CSAEM shall remain the principal coordination mechanism for reports involving online sexual abuse or exploitation of children and child sexual abuse or exploitation materials.

SEC. 14. *Duties of Parents, Guardians, and Schools.* — Parents and guardians shall have the primary responsibility to guide and supervise, in an age-appropriate manner, the internet and social-media use of children under their care.

Schools and other educational institutions shall adopt policies against cyberbullying, online harassment, and technology-facilitated abuse; assist children who report serious online risks; protect confidentiality; and coordinate with child-protection and law-enforcement authorities when required by law or necessary to protect a child.

Nothing in this Section shall impose criminal or administrative liability on a parent, guardian, or school solely because a child accessed a platform or violated an account restriction except when such parent, guardian or school failed to exercise due diligence of a good father of a family over such child.

SEC. 15. *Government Responsibilities.* — The Department of Information and Communications Technology shall be the lead implementing agency for the child online-safety and platform-accountability provisions of this Act, without prejudice to the statutory authority of the National Privacy Commission, the Department of Social Welfare and Development, the Department of Education, the Department of Justice, the Philippine National Police, the National Bureau of Investigation, and other concerned agencies.

The Department of Information and Communications Technology shall:

- (a) develop standards for platform compliance and privacy-preserving age assurance;
- (b) monitor compliance through documented and risk-based procedures;
- (c) conduct public education on child online safety;
- (d) provide technical assistance to covered platforms and concerned agencies;
- (e) publish an annual anonymized report; and
- (f) maintain a public registry of covered platforms, Philippine representatives, and responsible officers, subject to data-privacy laws.

The National Privacy Commission shall continue to exercise its powers under applicable data-privacy laws. The Department of Social Welfare and Development shall lead child-protection, psychosocial, referral, recovery, and rehabilitation services. The Department of Education, the Department of Justice, the Philippine National Police, the National Bureau of Investigation, the National Coordination Center against OSAEC and CSAEM, and other concerned agencies shall perform their respective functions under existing laws.

SEC. 16. *Administrative Sanctions.* — After written notice and a reasonable opportunity to be heard, the Department of Information and Communications Technology may impose the following sanctions on a platform that violates this Act or its implementing rules and regulations:

- (a) written warning and compliance order;
- (b) corrective action plan or independent audit;

- (c) administrative fine of not less than One million pesos (₱1,000,000.00) but not more than Ten million pesos (₱10,000,000.00) for the first violation;
- (d) administrative fine of not less than Ten million pesos (₱10,000,000.00) but not more than Fifty million pesos (₱50,000,000.00) for a second violation; and
- (e) administrative fine of not less than Fifty million pesos (₱50,000,000.00) but not more than One hundred million pesos (₱100,000,000.00) for a subsequent, willful, or grave violation.

For repeated, willful, or grave violations, the Department may order the revocation of a specific feature or function of the platform.

SEC. 17. *Criminal Liability.* — (a) A responsible officer shall be criminally liable when such officer had actual authority over the specific function or feature involved, actual knowledge of a specific and credible risk or written notice of that risk, or failed to perform a specific material duty within the prescribed period, where such failure directly *or* proximately caused imminent serious harm to a child or materially facilitated an offense punishable under applicable law. The penalty of imprisonment of not less than six (6) months but not more than six (6) years and a fine of not less than Five hundred thousand pesos (₱500,000.00) but not more than Five million pesos (₱5,000,000.00) shall be imposed upon such responsible officer.

- (b) The penalty of imprisonment of not less than six (6) months but not more than two (2) years and a fine of not less than One Hundred Thousand Pesos (₱100,000.00) but not more than Two Hundred Thousand Pesos (₱200,000.00) shall be imposed upon a parent, guardian, responsible person of a school, or the responsible officer of the platform for violation of Sec. 10 of this Act.

The penalties under this Section shall be without prejudice to liability under special laws and other applicable laws.

SEC. 18. *Protection of Children's Rights.* — Children shall retain their rights to privacy, freedom of expression, access to information, education, association, and participation in matters affecting them.

No child shall be denied access to health care, emergency assistance, government services, public-service information, or other essential services solely because the child does not possess a social-media account or declines to provide unnecessary personal information.

Age-assurance mechanisms shall not discriminate on the basis of disability, sex, gender, religion, ethnicity, socioeconomic status, nationality, or other protected status. The implementing rules and regulations shall provide reasonable accommodations and accessible alternatives.

SEC. 19. *Implementing Rules and Regulations.* — Within one hundred eighty (180) days from the effectivity of this Act, the Department of Information and Communications Technology, National Privacy Commission, Department of Social Welfare and Development, Department of Education, Department of Justice, Philippine National Police, National Bureau of Investigation, and National Coordination Center against OSAEC and CSAEM shall promulgate the implementing rules and regulations after public consultation.

The implementing rules and regulations shall include:

- (a) objective criteria for determining covered platforms;
- (b) standards for reasonable and proportionate age assurance;
- (c) privacy, security, retention, deletion, and breach-response requirements;
- (d) administrative procedures and sanctions;
- (e) reporting and referral procedures; and
- (f) safeguards against discrimination, overblocking, and unnecessary interference with lawful expression and access to information.

SEC. 20. *Periodic Review.* — Every three (3) years from the effectivity of this Act, the concerned agencies shall submit to Congress a joint report evaluating:

- (a) the effectiveness of the prohibition on personal social-media accounts for children below twelve (12) years of age;
- (b) the reliability, error rates, accessibility, and privacy impact of age-assurance methods;
- (c) platform compliance;
- (d) complaints involving privacy, discrimination, wrongful restrictions, and data breaches; and
- (e) the effect of this Act on children's safety, mental health, freedom of expression, access to information, and other rights of children.

SEC. 21. *Appropriations.* — The amount necessary for the initial implementation of this Act shall be charged against the current appropriations of the concerned agencies.

Thereafter, such sums as may be necessary shall be included in the annual General Appropriations Act.

SEC. 22. *Separability Clause.* — If any provision or part of this Act is declared unconstitutional or invalid, the other provisions not affected thereby shall remain in full force and effect.

SEC. 23. *Repealing Clause.* — All laws, decrees, orders, rules, regulations, and other issuances, or parts thereof, inconsistent with this Act are hereby repealed, amended, or modified accordingly.

SEC. 24. *Effectivity.* — This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in a newspaper of general circulation.

Approved.