

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

TWENTIETH CONGRESS
First Regular Session

House Bill No. **5931**



Introduced by Honorable Ma. Alana Samantha Taliño Santos

AN ACT STRENGTHENING CHILD ONLINE SAFETY IN SCHOOLS, MANDATING DIGITAL CITIZENSHIP EDUCATION, ANTI-CYBERBULLYING AND GROOMING PREVENTION, SAFE REPORTING SYSTEMS, EVIDENCE-PRESERVATION PROTOCOLS, AND SCHOOL-PLATFORM COORDINATION, AND FOR OTHER PURPOSES

EXPLANATORY NOTE

Children today live and learn in a digital world. The internet has created new ways to explore, connect, and learn, but it has also opened the door to serious risks that threaten the safety and well-being of young people. Incidents of cyberbullying, online grooming, doxxing, and the non-consensual sharing of private images continue to rise, often leaving children with lasting emotional and psychological harm.

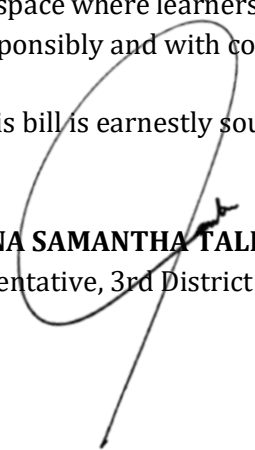
While the Department of Education has made progress in strengthening child protection in schools, many existing policies were designed for traditional forms of abuse and do not fully address the unique challenges of online harms. The digital environment has become an extension of the classroom, making it essential for schools to take a more active role in keeping learners safe both offline and online.

The proposed measure seeks to strengthen child online safety in schools by putting in place clear systems for prevention, reporting, and response. It requires the inclusion of digital citizenship and online safety lessons in the curriculum, regular training for teachers and school personnel, confidential reporting mechanisms for online abuse, and closer coordination between schools, government agencies, and online platforms. It also emphasizes the need for evidence preservation, psychosocial support, and data privacy safeguards to protect affected learners.

This bill complements the Anti-OSAEC and Anti-CSAEM Act, the Cybercrime Prevention Act, and other child protection laws by ensuring that online safety becomes a standard part of the education system. It aims to make every school a safe space where learners are not only protected but also empowered to navigate the digital world responsibly and with confidence.

In view of the foregoing, the immediate passage of this bill is earnestly sought.

MA. ALANA SAMANTHA TALIÑO SANTOS
Representative, 3rd District of Cotabato



Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

TWENTIETH CONGRESS
First Regular Session

House Bill No. **5931**

Introduced by Honorable Ma. Alana Samantha Taliño Santos

AN ACT STRENGTHENING CHILD ONLINE SAFETY IN SCHOOLS, MANDATING DIGITAL CITIZENSHIP EDUCATION, ANTI-CYBERBULLYING AND GROOMING PREVENTION, SAFE REPORTING SYSTEMS, EVIDENCE-PRESERVATION PROTOCOLS, AND SCHOOL-PLATFORM COORDINATION, 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 in Schools Act.”

SECTION 2. **Declaration of Policy.** — The State shall safeguard learners from online harms, including grooming, cyberbullying, doxxing, and non-consensual sharing of intimate images, by institutionalizing prevention, reporting, response, and coordination measures in schools. This Act complements the Anti-OSAEC and Anti-CSAEM Act, its IRR, and related child protection laws.

SECTION 3. **Definitions.** — For this Act:

(a) “Minor,” “child,” and “learner” refer to persons below eighteen (18) years enrolled in basic education, and those over eighteen (18) with special needs in basic education programs.

(b) “Cyberbullying” means repeated or severe acts using ICT that threaten, harass, humiliate, or intimidate a learner, including doxxing and incitement to self-harm.

(c) “Online grooming” means establishing trust or manipulation of a learner via ICT with intent to exploit, coerce, or engage the learner in sexual activity or other abuses, whether consummated or not.

(d) “School” includes public and private basic education institutions under DepEd supervision.

(e) “Trusted flagger” refers to an accredited entity or unit designated by DICT/CICC for expedited content action.

SECTION 4. **Digital Citizenship and Online Safety Curriculum.** — DepEd shall integrate age-appropriate digital citizenship, privacy, online safety, anti-grooming, and anti-cyberbullying modules across K–12, including bystander intervention and help-seeking.

SECTION 5. **Teacher and Personnel Training.** — Annual training for teachers, guidance personnel, child protection committees (CPCs), and ICT coordinators shall cover identification of risks, trauma-informed response, evidence preservation, referral pathways, and data protection.

SECTION 6. ***Parent and Learner Orientation.*** — Schools shall conduct at least semi-annual orientations on safe online conduct, reporting channels, mental health supports, and platform safety tools.

SECTION 7. ***Anti-Cyberbullying and Online Grooming Policy.*** — Each school shall adopt and publish a policy defining prohibited conduct, protected characteristics, confidential reporting channels, investigation timelines, proportional discipline, protective measures, and appeal procedures.

SECTION 8. ***Safe and Confidential Reporting Systems.*** — Schools shall maintain multiple reporting channels (in-person, anonymous digital, hotline). Reports implicating criminal conduct shall be promptly referred to law enforcement and DSWD, consistent with child protection laws.

SECTION 9. ***Evidence Preservation Protocols.*** — Schools shall implement protocols to:

- (a) Secure screenshots, URLs, hashes, and metadata where feasible;
- (b) Avoid unnecessary replication of sensitive images;
- (c) Preserve and transmit digital evidence to PNP-ACG/NBI-CCD upon request and coordinate with the Women and Children Protection Units (WCPUs);
- (d) Protect learner privacy and psychosocial well-being.

SECTION 10. ***Immediate Safety Measures.*** — Principals may issue no-contact directives, adjust schedules, and provide supervised access or safe spaces while investigations proceed, without prejudice to due process.

SECTION 11. ***School-Platform Memoranda of Understanding (MoUs).*** — DepEd shall develop model MoUs with major platforms and ISPs for:

- (a) Rapid takedown or restriction of content involving learners at risk;
- (b) Hash-matching to prevent re-uploads of reported materials;
- (c) Escalation lanes for schools and CPCs; and
- (d) Preservation of data for lawful requests under RA 10175 and RA 11930.

SECTION 12. ***Trusted Flagger and Emergency Escalation.*** — In coordination with DICT/CICC, DepEd may accredit divisions or CPCs as trusted flaggers for minor-involved harms to trigger 24-hour action windows, subject to safeguards and audit trails.

SECTION 13. ***Referral Networks.*** — Schools shall maintain updated referral directories for PNP-ACG, NBI-CCD, WCPUs, DSWD, and local psychosocial services, and use them in case management.

SECTION 14. ***Psychosocial Support and Accommodations.*** — Affected learners shall receive counseling, academic flexibility, and reintegration plans. Costs for urgent psychosocial services may be charged to MOOE or special funds as provided in the IRR.

SECTION 15. ***Data Protection.*** — Processing personal and sensitive data of learners shall observe privacy by design, data minimization, and strict access controls. Publication of reports shall exclude identifying details.

SECTION 16. ***School Child Protection Committees (CPCs)***. — CPCs shall oversee implementation, designate a cyber-safety focal person, ensure training, and submit incident summaries to the Schools Division Office (SDO) with privacy safeguards.

SECTION 17. ***Division and Regional Roles***. — SDOs and Regional Offices shall consolidate data, support complex cases, conduct compliance checks, and coordinate with DICT/CICC, PNP-ACG, NBI-CCD, and DSWD.

SECTION 18. ***DepEd Central Office Duties***. — DepEd shall issue the National Child Online Safety Manual; maintain escalation channels; negotiate platform MoUs; and publish anonymized annual reports on incidents, responses, and outcomes.

SECTION 19. ***Audits and Continuous Improvement***. — DepEd shall conduct periodic audits, disseminate lessons learned, and update modules and protocols based on evidence and technology changes.

SECTION 20. ***Relation to Other Laws***. — This Act shall be construed to supplement the Anti-OSAEC and Anti-CSAEM Act and its IRR, and coordinate with the Cybercrime Prevention Act procedures on data preservation and disclosure, without diminishing protections thereunder.

SECTION 21. ***Implementing Rules and Regulations (IRR)***. — Within six (6) months, DepEd, in coordination with DICT, CICC, DOJ, DSWD, DOH, PNP-ACG, NBI-CCD, and other agencies, shall promulgate the IRR, including templates for policies, protocols, and MoUs.

SECTION 22. ***Appropriations***. — The initial amount necessary for implementation shall be charged against current DepEd appropriations; thereafter, such sums as may be necessary shall be included in the annual General Appropriations Act.

SECTION 23. ***Separability Clause***. — If any provision is declared unconstitutional or invalid, the remainder shall remain in full force and effect.

SECTION 24. ***Repealing Clause***. — All laws, rules, and regulations inconsistent with this Act are repealed or modified accordingly.

SECTION 25. ***Effectivity***. — This Act shall take effect fifteen (15) days after its publication in the Official Gazette or a newspaper of general circulation.

Approved,