

Legal Education on Online Scams and the Risks of Using Artificial Intelligence at Special Program of SMP Muhammadiyah Al-Kautsar

Diana Setiawati*, Indah Maulani, Luthfiyyah Amalina Husna, Nuria Siswi Enggarani, and Novendya Nur Fitria Madyo

Universitas Muhammadiyah Surakarta, Surakarta, Indonesia

*Corresponding author email: ds170@ums.ac.id

Abstract

Generation Alpha has grown up in a digital ecosystem from an early age, but its technical skills have not been matched by an adequate understanding of the legal risks in cyberspace. Online scams, misuse of personal data, and the use of artificial intelligence (AI) websites that are not specifically regulated by statute pose real threats to students. This community service activity aimed to improve digital legal literacy among students at the Special Program of SMP Muhammadiyah Al-Kautsar, Sukoharjo, through a collaboration between the Faculty of Law of Universitas Muhammadiyah Surakarta and the Legal and Human Rights Council of the Sukoharjo Regional Board of 'Aisiyyah. The activity was conducted in five sessions from 10 June to 3 July 2026 and involved 150 students. The method used was participatory legal education, combining interactive lectures, discussions, and case simulations based on experiential learning. The topics covered included digital scam tactics, digital footprints and personal data protection, legal risks of using AI websites, digital ethics and legal responsibility, and case simulations. Evaluation was conducted qualitatively by observing participants' involvement and responses. The results indicate that presenting legal norms through cases familiar to students encouraged active participation and helped them connect everyday online behaviour with legal rights and obligations, particularly under the Personal Data Protection Law and the Electronic Information and Transactions Law. The author recommends that digital legal literacy be integrated sustainably into school student-development programs and evaluated using measurable instruments in future activities.

Submitted:

April 22, 2026

Accepted:

May 23, 2026

Published:

June 30, 2026

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

Keywords

Generation Alpha, Online Scams, Artificial Intelligence, Personal Data Protection, Digital Legal Literacy

Abstrak

Generasi Alpha tumbuh dalam ekosistem digital sejak usia dini, tetapi kecakapan teknis mereka belum diiringi pemahaman yang memadai tentang risiko hukum di ruang siber. Penipuan daring, penyalahgunaan data pribadi, serta pemanfaatan situs kecerdasan artifisial (artificial intelligence/AI) yang belum diatur secara khusus oleh undang-undang menjadi ancaman nyata bagi pelajar. Kegiatan pengabdian kepada masyarakat ini bertujuan meningkatkan literasi hukum digital bagi siswa SMP Muhammadiyah Al-Kautsar Program Khusus, Sukoharjo, melalui kolaborasi Fakultas Hukum Universitas Muhammadiyah Surakarta dengan Majelis Hukum dan HAM Pimpinan Daerah 'Aisyiyah Sukoharjo. Kegiatan dilaksanakan dalam lima sesi pada 10 Juni hingga 3 Juli 2026 dan diikuti oleh 150 siswa. Metode yang digunakan adalah penyuluhan hukum partisipatif dengan menggabungkan ceramah interaktif, diskusi, dan simulasi kasus berbasis pembelajaran eksperiensial. Materi mencakup modus penipuan digital, jejak digital dan perlindungan data pribadi, risiko hukum penggunaan situs AI, etika digital dan tanggung jawab hukum, serta simulasi kasus. Evaluasi dilakukan secara kualitatif melalui observasi partisipasi dan respons peserta. Hasil kegiatan menunjukkan bahwa penyajian norma hukum melalui kasus yang dekat dengan keseharian siswa mendorong keterlibatan aktif peserta, serta membranous siswa mengaitkan perilaku daring sehari-hari dengan hak dan kewajiban hukum, terutama menurut Undang-Undang Pelindungan Data Pribadi dan Undang-Undang Informasi dan Transaksi Elektronik. Penulis merekomendasikan agar literasi hukum digital diintegrasikan secara berkelanjutan ke dalam pembinaan siswa di sekolah, serta dievaluasi dengan instrumen terukur pada kegiatan berikutnya.

Kata Kunci

Perlindungan Hukum, Ketenagakerjaan, Kepatuhan Hukum dalam Bisnis, Keselamatan dan Kesehatan Kerja

Introduction

Advances in information technology have changed how children learn, play, and interact. A survey by the Indonesian Internet Service Providers Association found that internet penetration in Indonesia reached 79.5% in 2024, or approximately 221 million people, with young people representing a significant portion of users.¹ This

¹ Asosiasi Penyelenggara Jasa Internet Indonesia, "Survei Penetrasi Internet Indonesia 2024" (APJII, 2024), <https://survei.apjii.or.id/>.

group includes Generation Alpha, children born from around 2010 onward and the first generation to be born and grow up entirely amid digital devices, social media, and algorithm-based digital services.² In 2026, many members of Generation Alpha are of junior high school age.

Generation Alpha's technical fluency does not automatically translate into the ability to assess risks. Frameworks for classifying online risks to children distinguish content, contact, conduct, and contract risks, including scams, data exploitation, and harmful commercial practices.³ Research on victims of online fraud also shows that perpetrators exploit psychological factors such as promises of gain, trust, and time pressure, causing victims to make decisions without verification (Button et al., 2014). These patterns are particularly relevant to teenagers familiar with giveaways, online game-item transactions, and instant messaging.

These challenges have become more complex with the proliferation of generative artificial intelligence (AI) websites and applications. Technologies that enable the instant creation of text, images, audio, and video offer opportunities for creativity, but also create opportunities for copyright infringement, misuse of personal data, and the creation of manipulated content or deepfakes that can harm others.⁴ AI ethics literature emphasizes that AI should be used according to the principles of beneficence, non-maleficence, autonomy, justice, and explicability.⁵ UNICEF (2021) also highlights the need for special protection for children in AI policy.

From the perspective of positive law, Indonesia has several relevant legal instruments, including Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions (the EIT Law), Law No. 27 of 2022 concerning Personal Data Protection (the PDP Law), and Law No. 28 of 2014 concerning Copyright. However, AI has not yet been specifically regulated by statute. The government has issued Minister of Communication and Informatics Circular Letter No. 9 of 2023 on Artificial Intelligence Ethics, which serves as ethical

² Mark McCrindle and Ashley Fell, *Generation Alpha: Understanding Our Children and Helping Them Thrive* (Hachette Australia, 2021).

³ Sonia Livingstone and Mariya Stoilova, "The 4Cs: Classifying Online Risk to Children," *CO:RE Short Report Series on Key Topics* (Leibniz-Institut für Medienforschung | Hans-Bredow-Institut, 2021), <https://doi.org/10.21241/ssoar.71817>.

⁴ Robert Chesney and Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review* 107, no. 6 (2019): 1753–1820.

⁵ Luciano Floridi et al., "AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations," *Minds and Machines* 28, no. 4 (2018): 689–707, <https://doi.org/10.1007/s11023-018-9482-5>.

guidance for providers and does not stipulate sanctions. In these circumstances, users' legal awareness, especially that of children, becomes the first layer of protection. Legal awareness develops from knowledge of the law and understanding of its content to attitudes toward it and behaviour consistent with it.⁶ Legal education is therefore a strategic means of building this initial stage of legal awareness.

Several previous community service activities have addressed online scam prevention and digital literacy, including initiatives for rural communities⁷, youth groups⁸, and junior high school students in the context of e-commerce transactions⁹. These activities demonstrate the benefits of digital legal education; however, they generally have not combined online scams, personal data protection, and the legal risks of AI use into a single, progressive program for Generation Alpha. This activity seeks to address that gap.

Based on the foregoing, the Faculty of Law of Universitas Muhammadiyah Surakarta, together with the Legal and Human Rights Council of the Sukoharjo Regional Board of 'Aisyiyah, conducted legal education with the following objectives: (1) to improve students' ability to recognize online scam tactics; (2) to explain digital footprints and rights and obligations relating to personal data; (3) to introduce potential legal violations associated with AI websites; (4) to foster digital ethics and awareness of legal responsibility; and (5) to train students to make safe and ethical decisions through case simulations.

Method

This activity used a participatory legal education method. Participants were positioned as active learners rather than merely recipients of information. The approach was combined with experiential-learning principles, which view learning

⁶ Dewa Putu Tagel, "Kesadaran Hukum Masyarakat Pengguna Jalan Di Kota Denpasar," *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)*, 2013, 1–17.

⁷ Winarno Winarno et al., "Penyuluhan Bahaya Penipuan Online Sebagai Bentuk Peningkatan Literasi Digital Bagi Masyarakat," *Jurnal Pengabdian Nasional (JPN) Indonesia* 4, no. 2 (2023): 420–28, <https://doi.org/10.35870/jpni.v4i2.227>.

⁸ E Putri Silmina et al., "Meningkatkan Literasi Digital: Perlindungan Data Pribadi Dan Pencegahan Penipuan Online Di Lingkungan PRA Ngadisuryan," *Jurnal Pengabdian UntukMu NegeRI* 9, no. 2 (2025): 322–30, <https://doi.org/10.37859/jpumri.v9i2.9860>.

⁹ A Hanafi, A Awaliah, and A Kharismawan, "Literasi Hukum Dalam Transaksi E-Commerce Bagi Siswa Sekolah Menengah Pertama (SMP) Di Kota Palu," *Jurnal Altifani Penelitian Dan Pengabdian Kepada Masyarakat* 6, no. 5 (2026): 2869–80, <https://doi.org/10.59395/altifani.v6i5.1480>.

as a cycle of concrete experience, reflection, conceptualization, and active experimentation.¹⁰ This method was selected because junior high school students are more likely to understand legal norms when they are connected to everyday experiences.

Partners, Location, and Participants

The activity partner was the Special Program of SMP Muhammadiyah Al-Kautsar in Sukoharjo, Central Java, with the Legal and Human Rights Council of the Sukoharjo Regional Board of 'Aisyiyah (PDA 'Aisyiyah Sukoharjo) participating as a collaborative partner in community legal assistance. A total of 150 students participated, and all sessions were held at the partner school.

Implementation Stages

The activity consisted of three stages: preparation, implementation, and evaluation. Preparation included coordination with the school and the Legal and Human Rights Council of PDA 'Aisyiyah Sukoharjo, identification of the partners' needs and problems, preparation of materials, and scheduling. Implementation consisted of five educational sessions, each beginning at 9:00 a.m. Western Indonesian Time (WIB), as detailed in Table 1. Evaluation was conducted qualitatively by observing participation, questions, and responses during discussions, as well as the decisions students made during case-simulation sessions.

Table 1. Educational Topics and Speakers

No	Date	Topic	Speaker
1	Wednesday, 10 June 2026	Beware of Digital Scams: Recognizing Online Scam Tactics Targeting Young People	Diana Setiawati, S.H., LL.M.
2	Wednesday, 17 June 2026	Digital Footprints and Personal Data Security: Internet Users' Rights and Obligations in the Society 5.0 Era	Indah Maulani, S.H., M.H.
3	Wednesday, 24 June 2026	Between Creativity and Risk: AI Websites and Potential Legal Violations	Luthfiyyah Amalina Husna, S.H., M.H.
4	Wednesday, 1 July 2026	Digital Ethics and Legal Responsibility: Building Smart and Civil Conduct in Cyberspace	Dr. Nuria Siswi Enggarani, S.H., M.Hum.
5	Friday, 3 July 2026	Smart, Safe, and Ethical in the Digital World: Case Simulations	Novendya Nur Fitria Madyo

¹⁰ David A Kolb, *Experiential Learning: Experience as the Source of Learning and Development* (Prentice-Hall, 1984).

No	Date	Topic	Speaker
and Interactive Learning for Generation Alpha			

Source: Activity implementation documents, 2026.

Delivery Techniques

Each session consisted of three parts: (1) an opening prompt featuring a case or phenomenon familiar to students; (2) an interactive presentation connecting the phenomenon with relevant legal norms; and (3) discussion and questions and answers. The fifth session was specifically designed as a simulation. Students were presented with scenarios involving risky situations in the digital world and asked to determine appropriate actions based on what they had learned in the previous four sessions.

Results and Discussion

The activity was carried out as planned in five sessions from 10 June to 3 July 2026, with 150 students participating. The materials were arranged progressively, from identifying threats and understanding rights to assessing new-technology risks, developing ethical awareness, and practicing decision-making. This sequence was intended to build students’ understanding in stages, in line with the stages of legal awareness described in the literature.¹¹ The issues addressed in the session and the legal bases discussed are mapped in Table 2.

Table 2. Mapping of Educational Issues and the Legal Bases Discussed

Issue	Example of Risky Behaviour	Principal Legal Basis
Online scams	Sharing OTP codes; transferring money for fake prizes	EIT Law (Law No. 1 of 2024); Criminal Code (Law No. 1 of 2023)
Personal data and digital footprints	Uploading student ID photographs; sharing live location	PDP Law (Law No. 27 of 2022); EIT Law
Use of AI websites	Creating deepfakes of friends; uploading data to unclear AI websites	Copyright Law (Law No. 28 of 2014); PDP Law; Ministerial Circular No. 9 of 2023
Digital ethics and responsibility	Cyberbullying; spreading hoaxes	EIT Law; Child Protection Law (Law No. 35 of 2014)

Source: Compiled from the educational materials, 2026.

¹¹ Tagel, “Kesadaran Hukum Masyarakat Pengguna Jalan Di Kota Denpasar.”

The first session introduced online scam tactics commonly targeting teenagers, including social-media giveaways and fake prizes, scams involving the sale and purchase of online game items or accounts, phishing links impersonating trusted parties, and requests for one-time password (OTP) codes under the pretext that a code had been sent by mistake. Students were taught to recognize common warning signs: offers that seem too good to be true, pressure to act quickly, and requests for personal information or confidential codes. These patterns align with findings that scammers exploit the appeal of financial gain and time pressure to weaken victims' vigilance.¹²

From a legal perspective, students were introduced to the prohibition on disseminating false or misleading information that causes material losses to consumers in electronic transactions, as stipulated in the EIT Law, as well as the criminal provisions on fraud in the Criminal Code (Law No. 1 of 2023), which came into force on 2 January 2026. The emphasis was on two aspects: students may become victims who are entitled to protection, but they must also avoid becoming involved in scams, for example by lending their accounts or bank accounts to others.

The second session addressed personal data within the framework of Society 5.0, a concept of a human-centered society in which physical and cyberspace are closely integrated.¹³ Students were introduced to the concept of a digital footprint: every post, comment, and photograph can be stored, copied, and redistributed, even after its owner deletes it.

The legal material focused on the Personal Data Protection Law (PDP Law). This law classifies children's data as specific personal data and requires parental or guardian consent for the processing of children's personal data. Students were also introduced to the rights of personal data subjects, including the right to obtain information, correct data, erase data, and withdraw consent to data processing. In addition, the session discussed the right to request the deletion of irrelevant electronic information under the EIT Law. In practical terms, students were asked to evaluate risky habits such as uploading photographs of student identity cards, sharing their live location, and using public accounts without privacy settings.

¹² Mark Button et al., "Online Frauds: Learning from Victims Why They Fall for These Scams," *Australian & New Zealand Journal of Criminology* 47, no. 3 (2014): 391–408, <https://doi.org/10.1177/0004865814521224>.

¹³ Mayumi Fukuyama, "Society 5.0: Aiming for a New Human-Centered Society," *Japan SPOTLIGHT* 27 (2018): 47–50.

The third session discussed the use of generative AI websites and applications, which are increasingly popular among students. The material was not intended to prohibit AI use, but to develop students' ability to assess risks. At least three potential legal violations were discussed: (1) creating and distributing deepfakes of other people, which may harm victims' reputations and privacy¹⁴; (2) using other people's works without permission, which may implicate the Copyright Law; and (3) uploading photographs, voices, or personal data to AI websites whose operators and privacy policies are unclear, which may implicate the PDP Law.

The discussion also highlighted the absence of specific regulation. Minister of Communication and Informatics Circular Letter No. 9 of 2023 sets out AI ethics values, including inclusiveness, humanity, security, transparency, credibility, accountability, and personal data protection. However, a circular letter is not a generally binding legislative instrument and does not provide for sanctions. The government has also issued Government Regulation No. 17 of 2025 on the Governance of Electronic System Implementation for Child Protection, which imposes child-protection obligations on electronic system providers. Nevertheless, this regulation does not specifically govern responsibility in AI development and use. This situation reinforces the argument that user education on AI ethics must go hand in hand with the development of regulation.¹⁵

The fourth session connected legal literacy with character development. Ribble (2015) identifies ethics, rights and responsibilities, and security as components of digital citizenship.¹⁶ Students were encouraged to understand that cyberbullying, hate speech, spreading hoaxes, and distributing other people's photographs without permission are not merely breaches of etiquette but may also have legal consequences. In the context of Muhammadiyah schools, the material was also linked to moral values in social relations. Digital ethics was thus presented not as an unfamiliar set of rules, but as an extension of familiar manners and conduct into the digital space.

As children and legal subjects, students were also introduced to the principle that Indonesia's legal system provides special treatment for children, including children in conflict with the law. However, such special treatment does not erase the actual

¹⁴ Chesney and Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security."

¹⁵ UNICEF, "Policy Guidance on AI for Children," Version 2. (UNICEF Office of Global Insight and Policy, 2021).

¹⁶ Mike Ribble, *Digital Citizenship in Schools: Nine Elements All Students Should Know*, 3rd ed. (International Society for Technology in Education, 2015).

harm caused to victims. This point is important to ensure that students do not interpret their status as children as immunity from the law.

The fifth session applied the active-experimentation stage of the learning cycle. Students were presented with scenarios close to their everyday experiences, such as receiving a suspicious prize message, being asked for an OTP by an account claiming to belong to a friend or finding a friend's photograph manipulated using AI. Students were then asked to decide and explain what steps they would take. The response pattern promoted was to pause, verify, refrain from sharing the content, and report the incident to a teacher or parent.

Overall, observations during the activity showed that presenting material through concrete cases encouraged students to participate in discussions and question-and-answer sessions. Students also found it easier to connect everyday online behaviour with relevant legal norms. This finding is consistent with similar community service activities indicating that digital legal education based on real-life examples is well received. The added value of this activity lies in combining scams, personal data, and AI into one progressive program. The involvement of a community organization—the Legal and Human Rights Council of PDA 'Aisyiyah Sukoharjo'—also expanded access to legal assistance for students and families beyond the school environment.

This activity had several limitations. Evaluation was conducted qualitatively through observation, so changes in participants' knowledge and attitudes could not be measured quantitatively. In addition, the long-term impact on students' online behaviour was not monitored. Future activities are advised to use pre-tests and post-tests, attitude questionnaires, and periodic follow-up to measure whether behavioural changes are sustained.

Conclusion

The legal education activity on online scams and the risks of using artificial intelligence at the Special Program SMP Muhammadiyah Al-Kautsar was successfully conducted with the participation of 150 students. The participatory education method, combined with case simulations, helped students recognize online scam tactics. The activity also helped them understand their rights concerning personal data, assess the legal risks of using AI websites, and recognize their legal responsibilities for conduct in digital spaces. In the absence of a specific statute governing artificial intelligence (AI), legal literacy serves as an initial form of protection for children facing risks associated with digital technology. Schools are therefore advised to integrate digital legal literacy sustainably into student-

development programs, involve parents, and assess its impact using measurable evaluation instruments.

Acknowledgements

The authors would like to thank Universitas Muhammadiyah Surakarta for funding this community service activity, also extended to the Legal and Human Rights Council of the Sukoharjo Regional Board of 'Aisyiyah for its collaboration and support, to the principal and teaching staff of the Special Program of SMP Muhammadiyah Al-Kautsar for facilitating the activity, and to all students who participated actively.

References

- Button, Mark, Caroline M Nicholls, John Kerr, and Robert Owen. "Online Frauds: Learning from Victims Why They Fall for These Scams." *Australian & New Zealand Journal of Criminology* 47, no. 3 (2014): 391–408. <https://doi.org/10.1177/0004865814521224>.
- Chesney, Robert, and Danielle Keats Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review* 107, no. 6 (2019): 1753–1820.
- Floridi, Luciano, Josh Cowls, Monica Beltrametti, Raja Chatila, Patrice Chazerand, Virginia Dignum, Christoph Luetge, et al. "AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations." *Minds and Machines* 28, no. 4 (2018): 689–707. <https://doi.org/10.1007/s11023-018-9482-5>.
- Fukuyama, Mayumi. "Society 5.0: Aiming for a New Human-Centered Society." *Japan SPOTLIGHT* 27 (2018): 47–50.
- Hanafi, A, A Awaliah, and A Kharismawan. "Literasi Hukum Dalam Transaksi E-Commerce Bagi Siswa Sekolah Menengah Pertama (SMP) Di Kota Palu." *Jurnal Altifani Penelitian Dan Pengabdian Kepada Masyarakat* 6, no. 5 (2026): 2869–80. <https://doi.org/10.59395/altifani.v6i5.1480>.
- Indonesia, Asosiasi Penyelenggara Jasa Internet. "Survei Penetrasi Internet Indonesia 2024." APJII, 2024. <https://survei.apjii.or.id/>.
- Kolb, David A. *Experiential Learning: Experience as the Source of Learning and Development*. Prentice-Hall, 1984.
- Livingstone, Sonia, and Mariya Stoilova. "The 4Cs: Classifying Online Risk to Children." *CO:RE Short Report Series on Key Topics*. Leibniz-Institut für Medienforschung | Hans-Bredow-Institut, 2021. <https://doi.org/10.21241/ssoar.71817>.

- McCrindle, Mark, and Ashley Fell. *Generation Alpha: Understanding Our Children and Helping Them Thrive*. Hachette Australia, 2021.
- Putri Silmina, E, S Sarmini, U Umar, and H Herman. "Meningkatkan Literasi Digital: Perlindungan Data Pribadi Dan Pencegahan Penipuan Online Di Lingkungan PRA Ngadisuryan." *Jurnal Pengabdian UntukMu NegeRI* 9, no. 2 (2025): 322–30. <https://doi.org/10.37859/jpumri.v9i2.9860>.
- Ribble, Mike. *Digital Citizenship in Schools: Nine Elements All Students Should Know*. 3rd ed. International Society for Technology in Education, 2015.
- Tagel, Dewa Putu. "Kesadaran Hukum Masyarakat Pengguna Jalan Di Kota Denpasar." *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)*, 2013, 1–17.
- UNICEF. "Policy Guidance on AI for Children." Version 2. UNICEF Office of Global Insight and Policy, 2021.
- Winarno, Winarno, Y J Prasajo, M M Ibrahim, T A Joanida, N Saskya, and J Irgarenata. "Penyuluhan Bahaya Penipuan Online Sebagai Bentuk Peningkatan Literasi Digital Bagi Masyarakat." *Jurnal Pengabdian Nasional (JPN) Indonesia* 4, no. 2 (2023): 420–28. <https://doi.org/10.35870/jpni.v4i2.227>.