Indonesian Journal of Society Development (IJSD)
Vol.5, No.4, 2026: 393-404

Digital Literacy and Social Media Ethics Education for High School Students

Nani[1]*, Erlita Kurniawaty[2], Anah Furyanah[3]
Universitas Pamulang
Corresponding Author: Nani dosen01704@unpam.ac.id

A R T I C L E I N F O

Kata Kunci: Digital Literacy, Social Media Ethics, High School Students, Digital Security, Community Service

Received : 5 June 2026
Revised : 21 July 2026
Accepted: 22 August 2026

A B S T R A K

This community service program aimed to strengthen high school students' digital literacy, social media ethics, and basic digital security. The program was conducted at SMA Islam Cikal Harapan 1, South Tangerang, on 1–3 April 2026, using interactive lectures, group discussions, case studies, security practice, simulations, and question-and-answer sessions. The target cohort was 20 Grade X students; the appended attendance sheets contain 46 entries, indicating participation beyond the planned target, although the report does not reconcile the difference. Qualitative evaluation records improved awareness of information verification, respectful online communication, and personal-data protection. Presentation materials and a practical module were also produced for continued school use

DOI: https://doi.org/10.55927/ijsd.v5i4.40
E-ISSN: 2964-6006
https://journalijsd.my.id/index.php/ijsd/index

INTRODUCTION

Digital technologies and social media have become embedded in students' everyday lives. Platforms such as YouTube, Instagram, TikTok, WhatsApp, and Google support communication, information seeking, entertainment, self-expression, and school-related learning. These affordances can expand access to learning resources, strengthen creativity, and make interaction more flexible.

The benefits of digital participation are accompanied by risks. Adolescents may encounter hoaxes, disinformation, cyberbullying, privacy violations, hate speech, scams, identity theft, and excessive or unhealthy media use. The community-service report identifies these risks as particularly relevant to students who actively use social media but have not yet received systematic instruction in critical information evaluation, ethical communication, and personal-data protection.

Digital literacy is therefore understood in this article as more than technical ability. It includes the capacity to access, understand, evaluate, create, and share digital information critically and responsibly, together with ethical awareness and security practices. Prior works cited in the report emphasize the role of digital literacy in reducing digital inequality, supporting twenty-first-century learning, and encouraging productive creativity (Aisyah, 2021; Dewi et al., 2024; Febriani et al., 2024; Putri et al., 2023).

The partner institution was SMA Islam Cikal Harapan 1 in BSD City, South Tangerang. Initial observation and communication with the school indicated high social-media use alongside limited confidence in verifying information, maintaining respectful digital communication, and protecting personal data. The program consequently contributed a focused, school-based intervention that linked critical information skills with ethical conduct and practical account security.

This article reports the implementation and outcomes of the program. It describes the intervention stages, the participatory learning methods, the qualitative changes documented by the team, and the sustainability resources prepared for the school. Because the source report does not provide numerical pre-test and post-test scores, the results are presented as documented qualitative outcomes rather than as fabricated statistical estimates.

Problem Analysis and Intervention Rationale

The needs analysis in the source report points to a gap between access and capability. Students already encounter digital platforms frequently, yet frequency of use does not automatically produce the ability to judge credibility, communicate ethically, or manage security risks. This distinction shaped the program's rationale: the intervention was not designed to introduce technology as a novelty, but to improve the quality of students' existing digital participation.

The program also responded to the interconnected nature of digital risks. A student who forwards an unverified message may simultaneously contribute to disinformation, violate another person's privacy, and expose peers to harmful content. Likewise, a public post containing personal details may create both an ethical problem and a security vulnerability. Addressing literacy, ethics, and

security in a single learning sequence therefore offered a coherent response to the problems identified by the school.

A school-based setting was selected because teachers and school leaders can reinforce new habits after a short intervention. The report's sustainability plan—continued cooperation, mentoring, and reuse of the educational module—recognizes that responsible digital behavior is developed through repeated practice rather than a single information session.

IMPLEMENTATION AND METHODS

The activity followed a community-partnership model involving Universitas Pamulang and SMA Islam Cikal Harapan 1, Kencana Loka Block B.09 No. 1, Sector XII.1, BSD City, South Tangerang, Banten, Indonesia. The core activity was implemented over three days, Wednesday to Friday, 1–3 April 2026. The implementation team consisted of three lecturers—Nani as team leader, Erlita Kurniawaty as resource person, and Anah Furyanah as resource person—and two university students.

The report identifies Grade X students as the target audience and states that 20 students participated in the planned cohort. The appended attendance sheets, however, contain 46 student entries. Since no reconciliation is supplied, this article distinguishes the planned target (20) from the recorded attendance entries (46) and does not claim a verified final sample size beyond those source descriptions.

Table 1. Community-Service Problem-Solving Framework

Needs diagnosis	Learning intervention	Practice and reflection	Sustainability
Survey and school communication	Digital literacy, ethics, and security sessions	Discussion, case study, simulation, and feedback	Module and school follow-up

Implementation proceeded through four stages. First, the team surveyed the target group and communicated with school representatives to identify the setting, participant profile, and priority problems. Second, the team prepared learning materials, schedules, facilities, stationery, and task assignments. Third, the team delivered the face-to-face intervention through interactive lectures, discussion, question-and-answer, case analysis, and simple security simulations. Fourth, the team collected participant feedback and formulated a continuation plan with the school.

The learning content covered (1) the meaning and dimensions of digital literacy; (2) critical evaluation and verification of online information; (3) respectful language, privacy, and accountability in social-media communication; (4) cyberbullying and harmful content; and (5) strong passwords, two-step verification, suspicious links, online fraud, and protection of personal data.

Evaluation used pre-test and post-test questionnaires, observations of participation, discussion responses, and participant feedback. The report states that understanding increased after the program, but it does not include the instruments, item-level scores, sample-level means, or statistical tests. Accordingly, the present article reports direction and themes of change only.

Learning Design and Facilitation Sequence

The learning design combined explanation with application. Interactive lectures established a shared vocabulary, while group discussion allowed students to connect concepts with their own online routines. Case studies shifted the learning task from memorizing rules to making judgments about realistic messages, comments, screenshots, and links. The question-and-answer format then gave participants space to test their understanding and ask about situations not covered by the examples.

The facilitation sequence was intentionally progressive. Students first considered what digital literacy means and why verification matters; they then examined how online conduct affects other people; finally, they practiced basic security actions. This progression moved from interpretation, to responsibility, to protection. It also allowed the team to connect abstract ideas such as credibility and privacy with observable choices such as checking a source, revising a comment, or refusing to click a suspicious link.

The participatory approach is important for adolescent audiences because students bring prior experiences, peer norms, and platform-specific habits into the room. The report's description of active sharing suggests that the facilitators used those experiences as entry points rather than treating learners as passive recipients. In future sessions, the same principle can be strengthened through anonymous question cards, small-group role play, and student-generated examples.

Practical Module Outline

The module produced by the program can be organized into short units that a teacher can deliver independently or as a sequence. The outline below translates the reported materials into a reusable school resource while preserving the program's three core domains.

a. Unit 1—Digital participation: map the platforms students use, identify constructive uses for learning and creativity, and discuss the difference between access and responsible participation.
b. Unit 2—Checking information: practice a source–evidence–date–purpose check before accepting or forwarding a message; compare a supported claim with an unverified claim.
c. Unit 3—Ethical communication: revise potentially harmful comments, discuss privacy and consent, and identify responses to cyberbullying that protect the target and seek adult support.
d. Unit 4—Account and data security: review strong-password principles, two-step verification, privacy settings, suspicious links, and common online-fraud warning signs.

e. Unit 5—Personal action plan: each student writes two digital habits to start, one habit to stop, and one person or school channel to contact when a digital problem occurs.

A reusable module should also contain facilitator notes, a one-page student checklist, a short pre-test/post-test, and a feedback form. These additions would address the source report's main documentation gap while keeping the material practical for school use.

Table 2. Suggested Three-Day Implementation Schedule

Day	Focus	Core activities	Expected immediate product
Day 1	Digital literacy	Concept introduction, information-verification examples, group discussion	Student verification checklist
Day 2	Social-media ethics	Case study, dialogue on privacy and cyberbullying, Q&A	Revised ethical-response examples
Day 3	Digital security	Password and suspicious-link simulation, reflection, post-test	Personal security action plan

RESULTS AND DISCUSSION

Digital-Literacy Socialization

The opening session introduced digital literacy as a combination of access, comprehension, critical evaluation, responsible use, and safe participation. Facilitators used examples of information encountered on social media and asked students to consider the source, evidence, date, purpose, and emotional framing of a message before forwarding it. Students were reported to participate actively in discussion and question-and-answer exchanges.

The documented outcome was improved awareness that information should be verified before sharing. Students began to distinguish between receiving information and establishing its credibility, a distinction that is central to critical digital citizenship. This result is consistent with the report's literature review, which presents digital literacy as a foundation for critical thinking, communication, and problem solving in twenty-first-century education (Dewi et al., 2024; Krisnawati et al., 2022; Naila et al., 2021).

Social-Media Ethics Education

The second component addressed online communication norms, privacy, cyberbullying, harmful content, and the consequences of irresponsible posting. Rather than relying only on one-way explanation, the facilitators used interactive cases drawn from situations familiar to adolescents. Students discussed how

wording, screenshots, reposting, and comments can affect other people and how a digital trace can persist beyond the original moment.

The report records increased awareness of the need to use respectful language and to consider the impact of online behavior on others. Students also recognized that social-media participation carries social and potential legal consequences. In community-service terms, the intervention linked knowledge with character formation: students were positioned not merely as technology users, but as participants responsible for the quality of the digital environment.

Digital-Security Practice

The third component translated security principles into practical action. Students were introduced to strong-password characteristics, personal-data protection, suspicious links and websites, online-fraud risks, and basic account protection. A simple simulation asked participants to distinguish safer and weaker password patterns and to identify warning signs in questionable links.

The team reports that students became more aware of the risks of exposing personal information and of the need to protect social-media accounts. The practical emphasis matters because security knowledge is more likely to be retained when learners can apply it to familiar accounts and messages. The program therefore complemented conceptual literacy with concrete preventive behavior.

Participation, School Support, And Learning Climate

Participation was described as active across the sessions. Students shared experiences involving social-media use, information circulation, and everyday digital problems. These exchanges allowed facilitators to adapt explanations to authentic concerns and enabled peer learning. The school supported coordination, facilities, and supervision, which helped create a communicative and orderly learning climate.

The source report also documents a discrepancy between the planned cohort and the attendance sheets. The target was stated as 20 students, while 46 attendance entries were appended. This may indicate that the activity reached more students than planned, but the report does not provide a verified attendance reconciliation. Future implementations should record a single participant register, define inclusion criteria, and preserve matched pre-test/post-test identifiers.

Evaluation and Outputs

The report stated that pre-test and post-test questionnaires indicated improved understanding of digital literacy, social-media ethics, and digital security. Participants also reported that the activity helped them use social media more wisely and responsibly, and many expressed interest in recurring sessions. Because numerical scores are absent, the finding should be interpreted as a documented qualitative improvement rather than a quantified effect size.

Two practical outputs were produced: presentation materials and a simple educational module on digital literacy and social-media ethics. These outputs

extend the program beyond the three-day event by giving the school reusable content for classroom reinforcement, student orientation, or extracurricular activities. The output logic is aligned with previous studies cited in the report that frame literacy education as a continuing school responsibility (Inayah et al., 2023; Lubis et al., 2024; Ramadhani & Rosidah, 2023).

Outcome Interpretation by Learning Domain

In the information-verification domain, the central change was a shift from immediate acceptance toward a more deliberate checking stance. Students were encouraged to inspect source, evidence, timing, purpose, and emotional framing before forwarding information. Although the report does not quantify this shift, the repeated description of active discussion and improved awareness provides a plausible indication that students acquired a usable verification routine.

In the ethics domain, the program emphasized that online communication is still communication with real social consequences. Respectful language, privacy, and the prevention of cyberbullying were presented as everyday responsibilities rather than as abstract rules. The reported increase in awareness suggests that students could recognize how a comment, repost, or screenshot can affect another person and contribute to a healthier school digital culture.

In the security domain, practical examples made the consequences of weak passwords, public personal data, suspicious links, and online fraud more concrete. The simulation format supported procedural learning: students did not only hear that security matters, but practiced identifying safer choices. This is a useful complement to literacy education because secure behavior often depends on small, repeatable decisions.

Across domains, the program's value lies in integration. Critical evaluation helps a student decide whether information is trustworthy; ethics helps determine whether it should be shared and how; security awareness helps protect the account and people involved. The combined framework is particularly relevant to high school students whose learning, social interaction, and self-expression increasingly take place on the same platforms.

Table 3. Intervention Components and Documented Outcomes

Component	Main content	Method	Documented outcome
Digital literacy	Verification, hoaxes, critical use	Interactive lecture and discussion	Students more aware of checking information before sharing
Social-media ethics	Respect, privacy, cyberbullying, accountability	Case study and dialogue	Greater awareness of respectful and responsible communication

Digital security	Passwords, two-step verification, suspicious links, data protection	Practice and simulation	Improved awareness of account and personal-data risks
Reflection and feedback	Experience sharing and program evaluation	Q&A, observation, questionnaire	Positive response and interest in recurring activities

Table 4. Recommended Follow-Up Indicators for School Continuation

Domain	Short-term indicator	Follow-up evidence	Suggested frequency
Information literacy	Students apply a source-check routine	Short verification exercises or exit tickets	Monthly
Online ethics	Students recognize respectful and harmful communication	Scenario discussion and class reflection	Every term
Digital security	Students review account and privacy settings	Checklist completed with teacher guidance	Each semester
Healthy use	Students reflect on time, focus, and content exposure	Self-monitoring journal or advisory discussion	Monthly
School system	Digital-safety guidance is reused and updated	Module revision log and teacher feedback	Annually

Discussion of Contribution and Limitations

The principal contribution of the program is its integration of three dimensions that are often taught separately: critical information literacy, ethical communication, and personal security. For high school learners, the integration is pedagogically useful because the same social-media action—viewing, commenting, reposting, or clicking—can involve all three dimensions at once. The participatory format further positioned students' experiences as learning resources.

The evidence base remains limited by the reporting detail available in the source document. There are no numerical pre-test/post-test results, no instrument description, no demographic breakdown beyond the Grade X target, and no follow-up measurement of behavior. The attendance discrepancy should also be resolved in future reporting. These limitations do not negate the documented usefulness of the activity, but they do constrain claims about magnitude, generalizability, and long-term behavior change.

Implications for School Practice

For school leaders, the findings support treating digital literacy as a cross-cutting educational responsibility. The module can be positioned within homeroom guidance, information-technology learning, student counseling, or extracurricular activities. Such integration would reduce dependence on occasional external events and create regular opportunities for students to rehearse verification, respectful communication, and security practices.

For teachers, the most practical implication is the value of short, recurring exercises. A five-minute source-check routine, a discussion of one anonymized online scenario, or a monthly privacy checklist can reinforce the three-day intervention without requiring a new large event. Teachers can also model the behaviors expected from students by citing sources, protecting classroom data, and responding respectfully in school communication channels.

For parents and guardians, the program highlights the importance of dialogue rather than surveillance alone. Students benefit when adults ask how they judge information, what they do when they see cyberbullying, and which personal details should remain private. Consistent messages between school and home can make the program's recommendations easier to apply in daily life.

For the university team, the activity demonstrates a practical form of Tri Dharma collaboration. Future cycles can retain the accessible, participatory format while strengthening monitoring, documentation, and post-program mentoring. The partnership can also expand from awareness raising toward student-led digital ambassadors who help peers practice safe and ethical online behavior.

Sustainability and Scaling

The source report proposes continued collaboration and mentoring with the school. To operationalize this plan, the educational module should be treated as a living resource. Platform features, privacy settings, scams, and common forms of online harm change over time, so the school and university team should review examples and security guidance before each new cohort receives the material.

A feasible sustainability pathway is a train-the-teacher model. After the initial community-service event, one or more teachers can receive a facilitator guide, activity sheets, and a simple evaluation form. The teachers can then repeat selected activities during the school year, while the university team provides periodic refresher support and updates.

Scaling should preserve contextual relevance. A larger audience does not necessarily require longer lectures; it may require clearer group roles, peer facilitators, and differentiated cases for younger and older students. The attendance discrepancy in the source report also shows why scalable programs need a reliable registration and monitoring process from the outset.

The module and presentation materials provide a foundation for a local digital-citizenship package. With school approval, selected materials could be adapted for parent meetings, teacher workshops, or orientation for new students. Any expansion should maintain the same safeguards used in the original

program: no exposure of students' private data, no use of identifiable case details, and careful distinction between educational examples and real allegations.

Recommendations for Future Evaluation

Future implementations should retain the mixed-method approach but make it auditable. A short questionnaire can measure recognition of hoaxes, privacy risks, respectful language, password strength, and suspicious-link cues. The same instrument should be administered before and after the activity using anonymous participant codes so that change can be calculated without exposing identities.

Quantitative scores should be paired with qualitative evidence. Facilitators can record recurring misconceptions, questions, and examples of improved reasoning. A brief follow-up after four to eight weeks could examine whether students still use source checking, safer account practices, and respectful communication. These additions would allow the team to distinguish immediate comprehension from sustained behavior.

Reporting should also standardize participant information. The final report should state the planned target, registered participants, actual attendance, and the number of matched evaluation forms. Resolving these categories would prevent the 20-versus-46 discrepancy from limiting interpretation and would improve the credibility of future journal publications.

CONCLUSION AND RECOMENDATION

The community-service program at SMA Islam Cikal Harapan 1, South Tangerang, delivered a three-day educational intervention on digital literacy, social-media ethics, and digital security from 1 to 3 April 2026. Through lectures, discussion, case analysis, practice, simulation, and feedback, the program documented improved student awareness of information verification, respectful online communication, and protection of personal data. The school received presentation materials and a practical module to support continued learning.

The results should be understood as qualitative evidence because the report does not provide numerical pre-test and post-test data. The program's documented strengths were its relevance to students' daily digital experiences, its participatory learning climate, and the support of the partner school.

a. The school should repeat digital-literacy and social-media-ethics sessions periodically and integrate them into classroom or extracurricular activities.
b. Teachers and parents should provide complementary guidance and monitoring, especially on privacy, cyberbullying, scams, and healthy media-use routines.
c. Future programs should use a documented questionnaire, matched participant codes, and complete pre-test/post-test scores so that learning gains can be quantified.
d. The implementation team should reconcile target numbers with attendance records and document follow-up activities and behavioral indicators.

e. University–school collaboration should continue through refresher sessions, module updates, and mentoring for student digital ambassadors.

ACKNOWLEDGMENTS

The authors thank Universitas Pamulang, the Institute for Research and Community Service (LPPM), the Faculty of Economics and Business, and SMA Islam Cikal Harapan 1 BSD Tangerang for their institutional support. We also thank the school principal, teachers, students, lecturers, and university students who contributed to coordination, facilitation, participation, and documentation of the program.

REFERENCES

Aisyah, T. F. (2021). Literasi digital untuk meningkatkan minat baca siswa SMA pada pembelajaran daring. IQRA': Jurnal Perpustakaan dan Informasi.

Dewi, K. R., Subrata, H., & Puspita, A. M. I. (2024). Implementasi literasi digital di sekolah: Tinjauan pustaka sistematis. Jurnal Ilmiah Pendidikan Dasar, 10(1).

Febriani, W., Hasanah, M., Yupita, L., & Febriani, T. A. (2024). Literasi digital untuk meningkatkan kreativitas siswa MAS Lubuk Malako. Jurnal Pustaka Mitra: Pusat Akses Kajian Mengabdi Terhadap Masyarakat, 5(4).

Inayah, A., Matondang, A. H., Ritonga, D. P., & Nasution, N. S. (2023). Meningkatkan literasi digital siswa di sekolah dasar. Jurnal Pendidikan dan Ilmu Sosial (JUPENDIS), 2(3).

Krisnawati, N., Farradhillah, S. Q. A., Mariyam, S., Febrianti, I., Setianingsih, D., Iskandar, S., Majid, N. W. A., & Wulan, N. S. (2022). Literasi digital pada pembelajaran abad 21 di sekolah dasar. Enggang: Jurnal Pendidikan, Bahasa, Sastra, Seni, dan Budaya, 4(1).

Lubis, L. H., Febriani, B., Nasution, M. F., Siregar, U. D., & Salim, A. (2024). Pengembangan literasi digital di kalangan guru dan siswa: Kajian pustaka. Tarbiyah bil Qalam: Jurnal Pendidikan Agama dan Sains.

Naila, I., Ridlwan, M., & Haq, M. A. (2021). Literasi digital bagi guru dan siswa sekolah dasar: Analisis konten dalam pembelajaran. Jurnal Review Pendidikan Dasar, 7(2).

Putri, D. S., Soelfema, S., & Putri, L. D. (2023). Pendidikan literasi di era teknologi dalam mengatasi kesenjangan digital pada masyarakat. Jurnal Pustaka: Jurnal Bahasa dan Pendidikan, 5(1).

Ramadhani, E. N. F., & Rosidah, C. T. (2023). Pengaruh literasi digital terhadap keterampilan menulis teks deskripsi peserta didik sekolah dasar. Jurnal Pendidikan dan Pembelajaran Indonesia, 5(2).