

Educational Management Strategies to Address Information Security Challenges in the Use of Social Media in Learning Environments

¹Ahmad Jauhari Hamid Ripki

¹Program Studi Pendidikan Matematika, STKIP Kusumanegara, Indonesia

¹ahmadjauhari@stkipkusumanegara.ac.id

ABSTRACT

With the advancement of information technology, social media has become an integral part of daily life, including in the field of education. However, the use of social media in the learning environment is not exempt from information security challenges that can impact the effectiveness and sustainability of the learning process. This research aims to examine educational management strategies to address information security challenges in the use of social media in learning environments. The study employed an extensive review of existing literature through qualitative analysis to gain a comprehensive insight into the subject, covering the period from 2017 to 2023. The study's findings indicate that, in addressing the complexity of information security challenges related to the use of social media in learning environments, a holistic educational management approach is necessary. Awareness of risks, the development of clear policies, the selection of secure technologies, external collaboration, and continuous monitoring are key factors in creating a safe and innovative learning environment.

Keywords: Educational Management, Information Security, Social Media, Learning Environment

INTRODUCTION

This research summarises a background that builds on a growing understanding of the increasingly significant role of social media in learning contexts. In line with the rapid advancement of information technology, social media has become an integral element of everyday life, including in the realm of education (Fauzi et al., 2023). However, the integration of social media in learning environments cannot be separated from complex challenges related to information security, which can impact the effectiveness and sustainability of the learning process. Therefore, an in-depth understanding of these complex dynamics is essential to devise appropriate strategies to optimise the role of social media in supporting innovative and secure learning.

Firstly, it needs to be recognised that the existence of various social media platforms has provided easy access for learners to share information quickly and widely (Tarigan et al., 2023). While this offers positive potential in the context of learning, it also opens the door to risks such as leakage of personal information, dissemination of inappropriate content, and even potential cyber-attacks on learning systems. It is therefore imperative to design and implement education management strategies that are not only effective in responding to information security challenges, but are also able to ensure a learning environment that is secure, trusted and resilient to potential threats that could be detrimental to the overall learning process.

In addition, information security is increasingly crucial given the urgency of protecting learners' personal data, academic records and other sensitive information. In a broader context, information security management policies and practices in the education environment must be

carefully optimised to provide not only adequate, but also holistic protection against potential security threats (Kitsios et al., 2023). Given the dynamics of technological development and cyber intelligence, it is imperative that information security policies are proactive and aligned with the latest developments, to ensure the integrity, confidentiality and availability of information that forms the backbone of the learning process and data management in educational settings.

In addition, the complexity of managing information security is increasing along with the growing trend of online learning. This online learning phenomenon poses new challenges in maintaining data security, especially considering the intensive interaction between learners and educators through various social media platforms (Wut & Xu, 2021). Increased engagement through social media also brings potential risks of data leakage and cyber-attacks that can threaten the integrity of the learning system. Therefore, the focus of this research is not only on understanding the dynamics of online learning, but also on emphasising the need to design a holistic education management strategy. The strategy is geared towards integrating the use of social media with an optimal level of information security, creating an online learning environment that is not only academically effective but also safe and secure from potential security threats that may arise.

In the face of the complexity of the issues outlined, this research aims to comprehensively investigate the educational management strategies that can be implemented to address the information security challenges that arise in the use of social media in learning contexts. Through an in-depth analysis of the various aspects of this problem, this research intends to not only identify, but also detail and present innovative solutions. It is hoped that the results of this research will be able to generate evidence-based policy recommendations and concrete actions that can substantially improve the level of information security. In addition, it also seeks to formulate practical guidelines that can strengthen the effectiveness of learning through social media, ensuring that information security is not only a prerequisite but also a catalyst for the successful utilisation of social media in educational contexts.

LITERATURE REVIEW

Educational Management

Educational management refers to a series of planning, organizing, coordinating, implementing, and evaluating activities conducted by educational leaders and administrators to achieve educational goals effectively and efficiently (Rukman et al., 2023). In this context, educational management involves the management of human, financial, and physical resources within educational institutions, along with strategic decision-making focused on improving the quality of learning and achieving educational objectives (Azzaakiyyah et al., 2023). Educational managers must be able to design policies, organize learning processes, manage conflicts, and ensure the existence of a safe, inclusive, and innovative learning environment. Thus, educational management plays a crucial role in shaping the direction and effectiveness of the education system, positively impacting the development of learners, educators, and the community as a whole.

Information Security

Information security refers to a series of actions and policies implemented to protect the confidentiality, integrity, and availability of data or information within a system or organization. This includes efforts to prevent unauthorized access to information, prevent unauthorized changes or manipulation of data, and ensure the availability of information when needed (Kraugusteeliana, 2023; Manda HM & Abidin, 2023). Information security is not only focused on technical aspects but also encompasses human and process dimensions, such as involving users through security training, implementing appropriate access policies, and monitoring activities to detect potential security threats (Khando et al., 2021). With the increasing complexity of information technology and the frequent occurrence of security incidents, the importance of information security is increasingly emphasized in various sectors, including business, government, and education, to maintain trust, privacy, and smooth operations in information management.

Social Media

Social media refers to digital platforms that facilitate interaction, content sharing, and information exchange among users online. These platforms enable users to create, upload, and share various types of content, such as text, images, and videos, as well as participate in various forms of communication, ranging from comments, likes, to sharing other people's content (Ohara, 2023). The key characteristics of social media involve the concept of a social network, where users can connect with others, whether friends, family, or even unfamiliar individuals, through profile creation and building online relationships (Purnama & Asdlori, 2023). Social media has become an integral part of daily life, playing a crucial role in disseminating information, building communities, and facilitating social interactions at various levels, including personal, business, and education (Ausat, 2023). Popular social media platforms include Facebook, Twitter, Instagram, LinkedIn, and various other services that allow users to engage in broad and rapid digital activities (Azzaakiyyah, 2023).

Learning Environment

The learning environment encompasses the entire physical, social, and psychological context in which the learning process takes place (Closs et al., 2022). It includes classrooms, educational facilities, and physical infrastructure but also involves interactions among learners, educators, and other environmental elements. An effective learning environment should create conditions that support the growth and development of learners, facilitate positive social interactions, and provide visual stimuli and an inspirational learning environment (Richardson & Mishra, 2018). Additionally, psychological aspects such as safety, comfort, and emotional support also play a crucial role in shaping a conducive learning environment (Lateef, 2020). In the modern era, the learning environment also involves the use of technology and digital resources, including social media and online platforms, which can provide new dimensions in how learners interact and acquire knowledge. Therefore, the design of a holistic and adaptive learning environment is key to achieving effective learning goals and ensuring comprehensive development for learners.

RESEARCH METHOD

In this investigation, a qualitative approach is employed to thoroughly review the literature, aiming to explore strategies in education management that address information security challenges associated with the use of social media in learning environments. The study spans the critical period from 2017 to 2023 and utilizes this methodology to delve into scholarly works found in diverse academic journals, conference papers, and reputable sources available through Google Scholar. The literature exploration is guided by explicit search criteria formulated to include keywords related to Education Management, Information Security, Social Media, and Learning Environment. The inclusion of sources is based on their relevance to the research objectives, and any limitations, such as language constraints or publication biases, are transparently acknowledged.

The research progresses through distinct stages, commencing with the definition of a specific and relevant research topic and establishing a thorough understanding of the background and research objectives. Explicit search criteria are formulated to guide the literature exploration on Google Scholar, covering the timeframe from 2017 to 2023. Once search results are obtained, the researcher engages in a literature selection process, scrutinizing the abstracts and summaries of each identified article or source, and excluding literature lacking relevance or failing to meet the research criteria.

A meticulous examination of the chosen literature follows, focusing on identifying significant discoveries, concepts, theories, and trends inherent in the literature. The qualitative approach seeks to achieve a comprehensive understanding of the research subject. The findings from the literature review are then synthesized and elaborated upon by the researcher to construct a thorough understanding of the research topic. These findings are organized into a detailed research report with a structured and cohesive format, encompassing key discoveries, analyses, and profound interpretations.

This methodology, reliant on existing literature, has the potential to significantly contribute

to advancing theories, problem-solving, or decision-making across various scientific domains, particularly in the context of education management strategies to address information security challenges associated with the use of social media in learning environments. The structured methodology section provides a clear and coherent explanation of each stage of the research process, with subsections enhancing readability and ensuring a transparent and robust approach to the study.

RESULTS AND DISCUSSION

In the ever-evolving digital age, the utilisation of social media has become an indispensable element of everyday life, and this phenomenon also extends to the realm of education. While the integration of social media provides tremendous benefits in the context of learning, technological developments also bring complex challenges related to information security, especially when social media is integrated in the learning environment. Therefore, it is urgent to design and implement an educational management strategy that is not only meticulous but also purposeful, with the main objective of maintaining and improving the level of information security. This strategy is expected to not only address emerging security challenges, but also create a learning environment that is innovative, secure and responsive to the dynamics of technological change and social media development.

An essential first step in addressing the complexity of information security challenges in the education environment is to engage all stakeholders and increase their awareness and understanding. To achieve this, it is recommended to design and implement a comprehensive training programme and interactive workshops. By involving educators, students and parents, the aim is to provide an in-depth understanding of the information security risks that may arise with the use of social media (Zakaria et al., 2017). In addition, the programme was able to gain insight into best practices and preventative measures that can be effectively implemented to protect sensitive information (Borky & Bradley, 2019). In this way, it is hoped that efforts to improve the understanding of the entire education community will provide a solid foundation for establishing a proactive and information security-conscious attitude towards the use of social media in educational settings.

The development of a detailed and measurable information security policy is a crucial step in the effort to organise a learning environment that is safe and protected from potential data security risks (Tariq et al., 2023). Within this framework, it is necessary to formulate a policy that details key aspects related to the use of social media, ranging from limitations on use to the types of information that are allowed to be shared. This policy should also include concrete guidelines and procedures to be taken in dealing with various information security incidents, in line with technological developments and the dynamics of social media use. With these aspects in mind, the development of a comprehensive policy not only provides a clear framework for the use of social media in the learning environment, but also illustrates a serious commitment to information protection and a responsibility that the entire education community shares.

Within the framework of learning, specialised platform development efforts are becoming increasingly important with a special focus on information security aspects. These measures include selecting a platform that not only facilitates effective learning but also prioritises data security. Therefore, it is important to choose a platform that comes with integrated security features, which include data encryption and strict access control. Through the integration of these security features, the learning platform can serve as a secure and trusted environment, capable of protecting sensitive information from potential security risks (Gugueoth et al., 2023). In this way, the development of a dedicated learning platform that upholds information security not only supports effective learning processes, but also provides essential security assurance to ensure data integrity and confidentiality in modern learning contexts.

Developing partnerships with external parties, such as information security service providers or cybersecurity experts, is a strategy that is not only effective but also provides significant advantages in improving information security (Cremer et al., 2022). Collaboration with

these external experts allows schools to utilise their in-depth knowledge and expertise on the information security risks they may face. By working together, schools can more accurately detail and assess potential risks, and gain comprehensive insight into security strategies and solutions that are appropriate to their educational context (Dwivedi et al., 2023). Through this partnership, an inclusive framework is established, where the exchange of knowledge and resources between schools and external parties has the potential to result in innovative and up-to-date solutions for maintaining information security in the learning environment.

The importance of implementing an information security strategy lies not only in the initial steps, but also in the maintenance and continuous improvement through a systematic monitoring and evaluation system. By carrying out regular risk identification and evaluation processes, schools can build a strong foundation for adaptation and continuous improvement in information and technology governance. A sophisticated monitoring system will enable schools to detect potential threats or emerging security gaps over time, providing an opportunity to take preventive or corrective action before more serious problems occur (Šakić Trogrlić et al., 2022). Ongoing evaluation also provides an in-depth understanding of the effectiveness of the information security strategies implemented, enabling schools to refine and adapt their approach according to the evolving dynamics of the information and technology environment. Thus, the monitoring and evaluation system becomes the foundation for continuous improvement in maintaining information security in the educational environment.

Through a holistic approach, a number of important elements can be integrated to form a learning environment that is not only innovative but also optimised in terms of security. Firstly, awareness of information security risks and the importance of security in the use of technology is a strong foundation. Secondly, clear and comprehensive policies need to be designed and implemented to provide proper guidance in managing information and technology. Thirdly, secure technology, including the use of trusted platforms and software, data encryption, and sophisticated access control systems, ensures comprehensive protection of sensitive information. Fourth, collaboration with external parties such as information security service providers or cybersecurity experts is a valuable resource that can provide insights and solutions that match the latest security dynamics. Finally, careful monitoring through a continuous monitoring and evaluation system creates a cycle of continuous improvement, allowing schools to continuously adapt their security strategies and practices according to technological developments and changing security risks. By integrating all these elements, schools can shape a learning environment that is not only innovative but also safe for all parties involved.

CONCLUSION

Facing the complexity of information security challenges related to the use of social media in the learning context, a holistic educational management approach is deemed necessary. The key to creating a safe and innovative learning environment involves awareness of risks, the development of clear policies, the selection of secure technologies, external collaboration, and continuous monitoring. The implementation of these strategies is expected to help protect sensitive information, mitigate security risks, and ensure that the use of social media in the learning context yields optimal benefits. Therefore, schools can uphold data integrity, safeguard individual privacy, and ensure the sustainability of the learning process.

To address the complex challenges of information security in the use of social media in the learning environment, it is recommended to strengthen information security education programs for all stakeholders, including teachers, students, and parents. Continuous updates and improvements to information security policies are necessary to cover critical aspects such as usage limitations, types of shareable information, and responsive actions to security incidents. Intensive collaboration with information security experts and external institutions competent in cybersecurity can provide insights and solutions to overcome increasingly complex information security risks. The establishment of a sustainable monitoring and evaluation system is also crucial for proactively identifying and addressing information security risks. Through these steps, schools can create a

learning environment that is not only innovative but also carefully safeguards information security, nurturing a generation ready to face the challenges of the digital world wisely and securely.

REFERENCES

- Ausat, A. M. A. (2023). The Role of Social Media in Shaping Public Opinion and Its Influence on Economic Decisions. *Technology and Society Perspectives (TACIT)*, 1(1), 35–44. <https://journal.literasisainsnusantara.com/index.php/tacit/article/view/37>
- Azzaakiyyah, H. K. (2023). The Impact of Social Media Use on Social Interaction in Contemporary Society. *Technology and Society Perspectives (TACIT)*, 1(1), 1–9. <https://journal.literasisainsnusantara.com/index.php/tacit/article/view/33>
- Azzaakiyyah, H. K., Wanof, M. I., Suherlan, S., & Fitri, W. S. (2023). Business Philosophy Education and Improving Critical Thinking Skills of Business Students. *Journal of Contemporary Administration and Management (ADMAN)*, 1(1), 1–4. <https://doi.org/10.61100/adman.v1i1.1>
- Borky, J. M., & Bradley, T. H. (2019). Protecting Information with Cybersecurity. In *Effective Model-Based Systems Engineering* (pp. 345–404). Springer International Publishing. https://doi.org/10.1007/978-3-319-95669-5_10
- Closs, L., Mahat, M., & Imms, W. (2022). Learning environments' influence on students' learning experience in an Australian Faculty of Business and Economics. *Learning Environments Research*, 25(1), 271–285. <https://doi.org/10.1007/s10984-021-09361-2>
- Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 47(3), 698–736. <https://doi.org/10.1057/s41288-022-00266-6>
- Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., Baabdullah, A. M., Koohang, A., Raghavan, V., Ahuja, M., Albanna, H., Albashrawi, M. A., Al-Busaidi, A. S., Balakrishnan, J., Barlette, Y., Basu, S., Bose, I., Brooks, L., Buhalis, D., ... Wright, R. (2023). "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management*, 71, 102642. <https://doi.org/10.1016/j.ijinfomgt.2023.102642>
- Fauzi, F., Tuhuteru, L., Sampe, F., Ausat, A. M. A., & Hatta, H. R. (2023). Analysing the Role of ChatGPT in Improving Student Productivity in Higher Education. *Journal on Education*, 5(4), 14886–14891. <https://doi.org/10.31004/joe.v5i4.2563>
- Gugueoth, V., Safavat, S., & Shetty, S. (2023). Security of Internet of Things (IoT) using federated learning and deep learning — Recent advancements, issues and prospects. *ICT Express*, 9(5), 941–960. <https://doi.org/10.1016/j.icte.2023.03.006>
- Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, 106, 102267. <https://doi.org/10.1016/j.cose.2021.102267>
- Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability*, 15(7), 5828. <https://doi.org/10.3390/su15075828>
- Kraugusteeliana, K. (2023). A Study on Gender Roles in the Information Technology Profession and its Impact on Human Resources. *Technology and Society Perspectives (TACIT)*, 1(3), 104–111. <https://doi.org/https://doi.org/10.61100/tacit.v1i3.58>
- Lateef, F. (2020). Maximizing learning and creativity: Understanding psychological safety in simulation-based learning. *Journal of Emergencies, Trauma, and Shock*, 13(1), 5. https://doi.org/10.4103/JETS.JETS_96_19
- Manda HM, & Abidin, A. Z. (2023). The Role of Leadership in Managing Information Technology Change and its Impact on Organisational Human Resources. *Technology and Society Perspectives (TACIT)*, 1(3), 112–121. <https://doi.org/https://doi.org/10.61100/tacit.v1i3.59>

-
- Ohara, M. R. (2023). The Role of Social Media in Educational Communication Management. *Journal of Contemporary Administration and Management (ADMAN)*, 1(2), 70–76. <https://doi.org/10.61100/adman.v1i2.25>
- Purnama, Y., & Asdlori, A. (2023). The Role of Social Media in Students' Social Perception and Interaction: Implications for Learning and Education. *Technology and Society Perspectives (TACIT)*, 1(2), 45–55. <https://doi.org/10.61100/tacit.v1i2.50>
- Richardson, C., & Mishra, P. (2018). Learning environments that support student creativity: Developing the SCALE. *Thinking Skills and Creativity*, 27, 45–54. <https://doi.org/10.1016/j.tsc.2017.11.004>
- Rukman, W. Y., Urath, S., Harini, H., Ausat, A. M. A., & Suherlan, S. (2023). Philosophy Education as a Means of Developing Student Soft Skills. *Edumaspul: Jurnal Pendidikan*, 7(1), 281–286. <https://doi.org/https://doi.org/10.33487/edumaspul.v7i1.5458>
- Šakić Trogrlić, R., van den Homberg, M., Budimir, M., McQuistan, C., Sneddon, A., & Golding, B. (2022). Early Warning Systems and Their Role in Disaster Risk Reduction. In *Towards the "Perfect" Weather Warning* (pp. 11–46). Springer International Publishing. https://doi.org/10.1007/978-3-030-98989-7_2
- Tarigan, I. M., Harahap, M. A. K., Sari, D. M., Sakinah, R. D., & Ausat, A. M. A. (2023). Understanding Social Media: Benefits of Social Media for Individuals. *Jurnal Pendidikan Tambusai*, 7(1), 2317–2322. <https://jptam.org/index.php/jptam/article/view/5559>
- Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors*, 23(8), 4117. <https://doi.org/10.3390/s23084117>
- Wut, T., & Xu, J. (2021). Person-to-person interactions in online classroom settings under the impact of COVID-19: a social presence theory perspective. *Asia Pacific Education Review*, 22(3), 371–383. <https://doi.org/10.1007/s12564-021-09673-1>
- Zakaria, O., Zulhemay, M. N., Rashid, R. M., & Ganapathy, N. N. D. F. (2017). Engaging Information Security Awareness on Social Media: A Case Study of Secondary School Students. *Advanced Science Letters*, 23(8), 7601–7605. <https://doi.org/10.1166/asl.2017.9532>