Majority Science Journal (MSJ) Vol. 3 No. 4, November 2025
P-ISSN: 0000-0000; E-ISSN: 3025-1990
Available : https://jurnalhafasy.com/index.php/msj DOI: https://doi.org/10.61942/msj.v3i4.482

ETHICAL AND DATA SECURITY ANALYSIS IN THE IMPLEMENTATION OF GENERATIVE AI IN HIGHER EDUCATION ENVIRONMENTS

Aceng Haetami[1], Frhendy Aghata[2]
[1] Universitas Halu Oleo
[2] Universitas KH. Abdul Chalim

Inputed : October 16, 2025 *Revised : October 10, 2025*
Accepted : November 10, 2025 *Published : November 30, 2025*

Abstract

The rapid adoption of generative artificial intelligence in higher education has introduced significant pedagogical opportunities while simultaneously raising critical concerns regarding academic ethics and data security. This study aims to analyze ethical risks and data vulnerabilities associated with the use of generative AI by university students and lecturers, as well as to assess institutional readiness in establishing responsible AI governance. Using an analytical literature study with a descriptive qualitative approach, this research synthesizes empirical and conceptual findings from reputable international publications between 2015 and 2024. The findings indicate that generative AI poses threats to academic integrity through machine-generated plagiarism, reduced critical thinking, and algorithmic bias in learning processes. From a data security perspective, major risks include opaque data-storage policies, potential model memorization of sensitive information, and weak cybersecurity infrastructures in universities. Institutional readiness remains limited, marked by the absence of AI ethics guidelines, low AI literacy among academic communities, and inadequate monitoring mechanisms. This study recommends the development of generative-AI ethical guidelines, enhancement of digital literacy, improvement of data protection standards, and the establishment of AI governance committees within universities.
Keywords : *academic integrity, artificial intelligence, data security, ethics, higher education*

Citation :
Haetami, A., Aghata, F. 2025. Ethical and Data Security Analysis in The Implementation of Generative AI in Higher Education Environments. *MSJ: Majority Science Journal*, *3*(4), 177-186.
Coresponding Author:
Author name* Frhendy Aghata
Email* frhendy@uac.ac.id

1. Introduction

The development of generative artificial intelligence in recent years has created significant transformations in the higher education sector in various countries. Large language models such as ChatGPT, Bard, Claude, and Gemini have become the most rapidly adopted technologies in the history of education, with global usage among students reaching more than 60% in just the first year of their launch, according to an EDUCAUSE survey (Ahmed et al., 2024). Internationally, universities in the United States, Europe, and Asia have begun to integrate generative artificial intelligence into learning activities, assessment, research, and academic administration to improve efficiency and expand access to learning resources (Al Kautsar et al., 2024). However, this increase in usage raises serious ethical concerns, particularly regarding the transparency of algorithmic processes, bias in outputs, academic integrity, and the security of personal data of students and lecturers who interact with generative AI systems (Dabis & Csáki, 2024).

In Indonesia, the development of generative artificial intelligence use in higher education has also increased significantly along with the increase in student digital literacy. A survey by the Indonesian Internet Service Providers Association shows that more than 35% of young internet users have used generative AI platforms in 2023 to complete academic assignments (APJII, 2023). Major universities such as the University of Indonesia, Gadjah Mada University, and the Bandung Institute of Technology have begun to explore

opportunities for integrating generative AI into learning, although most do not yet have comprehensive data security and ethics policies to regulate the use of this technology. This condition shows that the higher education ecosystem in Indonesia is in a phase of rapid adoption but is not yet accompanied by adequate technology governance mechanisms, particularly regarding issues of student data protection, the risk of personal information leaks, and the ethical implications for the integrity of the academic process (Arista et al., 2024).

Globally, the issue of generative AI ethics in higher education is becoming an important concern. UNESCO (2023) emphasizes that the use of generative AI without a strong ethical framework has the potential to create technological dependence, exacerbate digital inequality, and threaten student intellectual autonomy. In addition, generative AI models collect large amounts of user interaction data that can be used to retrain models, posing risks to academic privacy and sensitive data security (Fatmadiwi et al., 2025). Vulnerability to data leaks is increasing because universities often lack the technical capacity of large technology companies to protect the digital data of their academic community. This is in line with Maulana (2025) finding that generative AI training datasets are often obtained from open sources that lack privacy verification mechanisms, making the potential for personal data breaches a crucial issue in its application.

Apart from data security issues, another challenge that has emerged is academic integrity. The availability of generative AI allows students to produce essays, data analyses, and even computer programs with little effort, raising concerns that the use of this technology could blur the line between students' original work and algorithm outputs. According to Torres et al., (2023), students' increasing reliance on generative AI can reduce their level of conceptual understanding, weaken their critical thinking skills, and create the risk of machine-generated plagiarism, which is difficult to detect using conventional plagiarism checkers. On the other hand, lecturers also face the challenge of adapting their teaching and assessment methods to remain relevant in an era when AI can generate sophisticated answers.

Another problem is algorithmic bias. Generative AI models are built using large-scale datasets that are often dominated by certain cultural and linguistic representations, so the outputs tend to reflect these biases. This has the potential to create inequality in the learning context, especially for students from minority cultural groups or from different linguistic backgrounds (Olohunfunmi & Khairuddin, 2024). In the context of Indonesia, with its cultural and linguistic diversity, algorithmic bias can create new barriers to efforts to achieve inclusive higher education. Therefore, a deep understanding of the ethical impact of generative AI on learning quality, access to education, and student representation is needed.

The urgency of this research is even greater given that higher education institutions are at a crossroads between the need to adopt new technologies and the obligation to maintain the integrity of the academic process. Educational institutions must ensure that the use of generative AI does not compromise ethical standards, student data privacy, and the principle of fairness in the academic evaluation process. According to Resky & Suharyat (2024), universities need to develop an AI policy framework that not only emphasizes technological innovation but also prioritizes moral principles such as transparency, accountability, and inclusivity. However, to date, many higher education institutions do not have clear guidelines on generative AI ethics, so its implementation is sporadic and depends on the policies of each faculty or lecturer.

In the context of scientific research, there are a number of research gaps that indicate the need for new studies related to ethics and data security in the implementation of generative AI in higher education. First, a study titled “Generative AI in Higher Education: A Framework for Academic Integrity” by Kasneci et al. (2023) focuses on the aspect of academic integrity but does not discuss the issues of data security and student privacy protection in the use of generative AI. Second, the study “Ethical Risks of AI-Assisted Learning Tools” by Floridi & Chiriatti (2020) highlights the epistemological issues of AI use, but does not examine in depth how higher education institutions can develop comprehensive risk management policies. Third, the study “AI Adoption in Universities: Opportunities and

Challenges" by Tlili et al (2023) discusses the opportunities for generative AI integration, but does not conduct an empirical analysis of the threats of data leaks and algorithmic bias against student populations in developing countries such as Indonesia. These three studies are important, but they do not provide an integrated perspective that combines ethical issues, data security, academic confidentiality policies, and the social context of students, thus creating a gap in research that needs to be filled.

Based on this research gap, this study offers a novelty in the form of an in-depth analysis that simultaneously integrates the dimensions of ethics and data security in the context of higher education in Indonesia, by reviewing how generative AI affects academic integrity, digital privacy, and institutional governance. The novelty of this research also lies in its interdisciplinary approach, which combines perspectives on educational technology, artificial intelligence ethics, and educational cybersecurity literature.

Therefore, the purpose of this study is to comprehensively analyze ethics and data security in the implementation of generative artificial intelligence in higher education, by assessing its implications for academic integrity, student privacy, and the readiness of higher education institutions in developing responsible AI governance.

2. Method

This study uses a descriptive qualitative method with an analytical literature study approach, which focuses on a systematic review of empirical and conceptual findings discussing ethics and data security in the use of generative artificial intelligence in higher education. This method was chosen because the issues studied are related to ever-evolving technological phenomena and require in-depth understanding through critical synthesis from various scientific sources. According to Snyder (2019), analytical literature studies allow researchers to evaluate diverse empirical findings, identify conceptual patterns, and draw important conclusions for the educational context. The research data was sourced from reputable journal articles indexed by Scopus and Web of Science, publications from global institutions such as UNESCO and the OECD, and digital education research reports released between 2015 and 2024.

The literature collection process was carried out in three main stages, namely identification, selection, and thematic analysis. In the identification stage, researchers searched for relevant articles using keywords such as generative AI, data security in higher education, AI ethics, and academic integrity. In the selection stage, literature was selected based on topic relevance, scientific novelty, and methodological quality as suggested by Xiao and Watson (2019). Articles that were not relevant to the context of higher education or did not discuss ethical and data security implications were eliminated. Furthermore, in the analysis stage, researchers used thematic analysis techniques to group findings into categories: academic integrity, data privacy and security, algorithmic bias, and institutional readiness. This approach provides space for critical interpretation of the main patterns and issues that emerge from the literature.

This study does not aim to produce statistical generalizations, but rather to provide a conceptual and evaluative understanding of the ethical and data security risks in the implementation of generative AI in higher education. Using a rigorous thematic analysis strategy, this study produced an argumentative construction that maps the main challenges and technological governance needs in higher education institutions, as also recommended by Braun and Clarke (2021). The results of the analysis were then abstracted to compile conceptual recommendations relevant to higher education institutions in Indonesia in designing policies for the safe, ethical, and inclusive use of generative AI.

3. Results and Discussion

Academic Integrity and Ethical Risks in the Use of Generative AI in Higher Education

The use of generative artificial intelligence in higher education has brought about significant changes in the way students and lecturers interact with information, complete academic assignments, and produce scientific work. However, behind the potential for

P-ISSN: 0000-0000; E-ISSN: 3025-1990
Available : https://jurnalhafasy.com/index.php/msj DOI: https://doi.org/10.61942/msj.v3i4.482

increased efficiency and creativity, there are major challenges regarding academic integrity, which is one of the main pillars of the higher education ecosystem. Academic integrity includes scientific honesty, originality of work, fairness in evaluation, and respect for the learning process. The availability of generative AI capable of producing text, code, statistical analysis, and even visual designs in seconds has blurred the line between students' original work and machine-generated content, creating a potential for abuse that cannot be ignored (Al Kautsar et al., 2024).

One of the main risks to academic integrity is the rise of machine-generated plagiarism. Traditional text-matching plagiarism detection methods such as Turnitin are no longer adequate because generative AI can produce completely new output that is not identical to any source. Torres et al.,'s (2023) study shows that more than 70% of academic detection tools are unable to identify text generated by generative language models, mainly because these algorithms are designed to detect copying, not the generation of new content. This indicates that higher education institutions must develop new approaches that assess the learning process of students, not just the final outcome in the form of written documents.

Beyond the potential for plagiarism, there are concerns that the use of generative AI may reduce students' ability to think critically and process information independently. Students who rely on AI to compose essays, answer questions, or perform risk analysis lose the opportunity to develop metacognitive, argumentation, and academic literacy skills. Resky & Suharyat (2024) note that students who are overly dependent on AI-based tools show a decline in cognitive motivation and quality of understanding of learning materials. This risk highlights the need for new pedagogy that emphasizes the use of AI as a supporting tool, not as a substitute for the thinking process.

At the lecturer level, the use of generative AI also presents challenges in assessing learning outcomes. In situations where students can produce high-quality assignments with the help of AI, lecturers face difficulties in distinguishing between work that truly reflects student ability and work that is largely generated by algorithms. This raises the potential for unfairness in academic evaluation. Arista et al., (2024) show that lecturers who are unfamiliar with the linguistic patterns of generative AI have difficulty identifying content elements that are machine-generated, resulting in inaccurate assessments. This situation highlights the need to improve faculty capacity in AI literacy and understanding of how the technology works.

Another important ethical issue in the use of generative AI in higher education is algorithmic bias, which can affect the learning process. Generative AI models are trained using large datasets that often reflect cultural, linguistic, and demographic representation imbalances. Consequently, AI output may reflect certain biases that could potentially disadvantage students from underrepresented backgrounds. Buolamwini and Gebru (2018) show that AI models are often biased toward certain racial groups in image recognition; in an educational context, similar biases can arise in the form of task interpretation, content recommendations, or automated academic guidance processes. Even in the Indonesian context, language bias is a critical issue because most models are trained using English-language data, limiting AI's ability to understand the local context, which can hinder the learning process of students who use Indonesian in their daily lives.

Furthermore, ethical risks arise when students use generative AI for purposes that are not in line with the principles of academic integrity, such as circumventing the assessment process or generating answers without substantial understanding. Research by Floridi and Chiriatti (2020) highlights the phenomenon of epistemic opacity, a condition in which users do not understand how and why AI produces certain outputs. When students accept AI outputs as truth without verification, the educational process becomes distorted. Thus, the use of generative AI can shift the focus of learning from the pursuit of knowledge to the pursuit of instant results.

On the institutional side, universities face an ethical dilemma between encouraging innovation and maintaining academic integrity. Higher education institutions have historically functioned as guardians of scientific standards and academic quality, so the unregulated use

P-ISSN: 0000-0000; E-ISSN: 3025-1990
Available : https://jurnalhafasy.com/index.php/msj DOI: https://doi.org/10.61942/msj.v3i4.482

of generative AI could threaten the legitimacy of the academic process. According to Mayasari et al., (2025), several universities in Europe and America have established AI ethical guidelines that include principles of transparency of use, attribution obligations when using AI tools, and restrictions on use in certain tasks. However, many institutions in developing countries, including Indonesia, do not yet have formal guidelines, leading to inconsistencies in policies among faculties and study programs.

It is undeniable that generative AI also opens up opportunities for ethical and positive use, such as helping students understand difficult concepts, supporting students with special needs, and accelerating the research process. However, these opportunities can only be exploited if the risks to academic integrity are properly managed. This requires a balance between technology adoption and the establishment of an ethical framework that ensures that the use of generative AI does not sacrifice the main objectives of higher education, namely the development of students' intellectual capacity and academic character.

Considering these various risks, it can be concluded that academic integrity is a central issue that needs serious attention in the implementation of generative AI in higher education. Universities need to establish clear usage limits, provide AI literacy training to lecturers and students, and develop alternative assessment strategies that can minimize the potential misuse of generative AI. This approach is important to ensure that generative AI is used as a tool that strengthens the learning process, not as a means of undermining academic ethics.

Data Security and Privacy Risks in the Implementation of Generative AI in Higher Education

The increased use of generative artificial intelligence in higher education cannot be separated from the increasingly complex issues of data security and digital privacy protection. Generative AI technology operates through large machine learning models trained using massive amounts of data, and most user interactions including those of students and faculty have the potential to become part of the input data used for further training. Jin et al., (2025) assert that the characteristics of machine learning-based AI blur the lines between input data, training data, and output, thereby significantly increasing the risk of data leaks and exposure of sensitive information. In the context of higher education, where academic interactions often involve personal information, student assignment data, research designs, and evaluation results, threats to academic confidentiality become an urgent issue that must be managed seriously.

One of the fundamental problems in data security is the nature of commercial generative AI platforms that operate with data collection policies that are not fully transparent. Research by Jin et al., (2025) shows that most generative AI providers have data usage clauses that allow the system to store user input for model evaluation, algorithm improvement, or dataset retraining purposes. This poses a significant risk to students and lecturers who use AI services to complete assignments, upload research texts, or enter sensitive information that should not be accessed by other parties. When this data is stored on the servers of global technology companies, universities lose control over the distribution and security of academic data. In some cases, academic data even has high intellectual value that should be protected, such as research that is being developed or exam materials.

Furthermore, data security risks also arise from the potential for data leakage that can occur when generative AI model outputs contain fragments of personal information or content that resembles training data. Mayasari et al., (2025) found that large language models can “spit out” pieces of training data when prompted with certain prompts, especially if the data appears frequently in the dataset. Although no similar cases have been found in the context of higher education in Indonesia, this potential remains a serious threat if students or lecturers enter academic data into the system. This risk is compounded by the fact that most universities do not have internal policies regarding what types of data may or may not be entered into generative AI platforms, resulting in the unregulated use of AI without adequate protection.

P-ISSN: 0000-0000; E-ISSN: 3025-1990
Available : https://jurnalhafasy.com/index.php/msj DOI: https://doi.org/10.61942/msj.v3i4.482

At the institutional level, the issue of data security becomes even more complicated because many universities do not yet have information security management systems that are compatible with international standards such as ISO/IEC 27001. Arista et al. (2024) note that the majority of universities in Indonesia only rely on basic security systems and have not developed specific protocols for user interaction data with generative AI. As a result, universities are unable to provide adequate security guarantees against potential data theft, personal information leaks, or academic exploitation by external actors. With the increasing adoption of digital technology, higher education institutions have the potential to become targets of cyber attacks that exploit structural vulnerabilities in university information technology systems.

In addition, the use of generative AI requires universities to consider compliance with applicable data protection regulations at both the national and international levels. A study by Wibowo (2025) shows that non-transparent data governance mechanisms have the potential to violate digital ethics principles such as data minimization, purpose limitation, and informed consent. Although Indonesia already has a Personal Data Protection Law (2022), its implementation in the higher education sector is still in its early stages, so many universities have not yet systematically applied data security principles, such as the obligation of data controllers to secure the collection, processing, and storage of student data used in AI systems.

To provide a more structured overview of privacy and data security risks, the following table summarizes the main challenges arising from the implementation of generative AI in higher education:

Table 1. Data Security and Privacy Risks in the Use of Generative AI in Higher Education

Risk Category	Description	Implications for Higher Education
Data storage uncertainty	User inputs may be stored or used for model training	Loss of control over academic data; potential privacy breaches
Model memorization	AI models may reproduce sensitive fragments from training data	Leakage of student assignments or research material
Weak institutional policies	Universities lack guidelines on ethical AI use	Unregulated data handling and inconsistent data protection
Cybersecurity vulnerabilities	IT systems not aligned with international security standards	Increased exposure to attacks and data theft
Ambiguous consent mechanisms	Users unaware of how data is collected and used	Violation of privacy principles and legal compliance

The table shows that data security issues lie not only in the technical aspects of AI technology, but also in the weaknesses of higher education institution governance. If universities do not implement clear policies, students and lecturers may unknowingly enter sensitive data into unsupervised generative AI systems. The risk increases when users do not understand that their interactions with generative AI leave digital traces that can be processed by third parties. This is in line with Kasman & HB (2025) findings on data colonialism, a phenomenon where user data is collected, stored, and exploited by entities with technological power.

Data security challenges are also closely related to institutional trust. Students tend to believe that all technologies used on campus have been verified for security, so they are more likely to freely enter academic or personal data into generative AI platforms. However, when data leaks or information misuse occur, universities often find it difficult to mitigate the

P-ISSN: 0000-0000; E-ISSN: 3025-1990
Available : https://jurnalhafasy.com/index.php/msj DOI: https://doi.org/10.61942/msj.v3i4.482

situation because they do not have adequate documentation on technology use or do not monitor AI usage patterns on campus in a structured manner (Marlin et al., 2023). The inability of institutions to protect the digital data of the academic community can damage their academic reputation and lead to mistrust of technology use.

Considering these various risks, it is clear that data security is one of the key components in the governance of generative AI use in higher education. Efforts to strengthen data security must be carried out through the development of internal guidelines, increased information technology capacity, and a deep understanding of the privacy policies of generative AI platforms. Universities must ensure that the use of this technology does not sacrifice the privacy rights of students and lecturers, and does not create structural vulnerabilities to academic data leaks.

Governance and Institutional Readiness of Higher Education in the Implementation of Generative AI

The implementation of generative artificial intelligence in higher education depends not only on the ability of students and lecturers to use it ethically, but also on institutional readiness to provide clear, measurable, and sustainable governance. Generative AI governance includes internal policies, digital infrastructure capacity, human resource competencies, and mechanisms for monitoring the use of technology on campus. According to Mayasari et al., (2025), universities act as controllers of academic policy as well as guardians of ethics in the use of new technology, so institutional readiness is a determining factor in whether the adoption of generative AI brings benefits or causes academic and privacy problems.

However, current conditions show that the majority of universities, both globally and in Indonesia, do not yet have comprehensive policies regarding the use of generative AI. A UNESCO study (2023) found that less than 10% of higher education institutions worldwide have adopted written and structured policies on the use of AI in learning and assessment processes. A similar situation is found in Southeast Asia, where most universities use generative AI on an ad hoc basis without clear ethical guidelines or data policies (Arista et al., 2024). The lack of such policies means that the use of generative AI takes place without adequate institutional control and often depends on the personal interpretation of lecturers or faculty.

Generative AI governance requires a policy framework that includes the principles of transparency, accountability, privacy, and fairness. Transparency is necessary so that students and lecturers understand the limitations of AI use and what types of interactions are considered ethical. The OECD (2021) emphasizes that AI policies in higher education must include clarity of use and attribution, including the need to state that certain texts or analyses were assisted by AI. Without the principle of transparency, there is ambiguity between original work and machine-generated content, which can ultimately undermine academic authenticity. Universities must also establish accountability mechanisms, including sanctions for AI misuse and procedures for handling academic integrity violations involving generative technology.

Digital infrastructure readiness also plays an important role in supporting generative AI governance. Many universities, especially in developing countries, still experience limitations in digital security infrastructure, data storage capacity, and adequate network quality. Arista et al. (2024) note that most universities in Indonesia are in the early stages of developing a digital security foundation and do not yet have data traffic monitoring protocols that meet international standards. In the context of generative AI use, these infrastructure limitations can make it difficult to protect student data, audit AI use, or monitor user activity internally. Inadequate infrastructure also increases the risk of cyber vulnerabilities that can be exploited by external parties.

In addition, institutional readiness is largely determined by the technological literacy of stakeholders, especially lecturers and educational staff. Lecturers play a central role in guiding the ethical use of generative AI in the classroom, determining the limits of use in

P-ISSN: 0000-0000; E-ISSN: 3025-1990
Available : https://jurnalhafasy.com/index.php/msj DOI: https://doi.org/10.61942/msj.v3i4.482

assignments, and assessing whether students have used AI responsibly. However, research by An et al., (2025) shows that many lecturers do not yet have a deep understanding of how generative models work, making it difficult for them to identify potential biases, misuse, or inaccuracies in AI outputs. The lack of technological literacy among educators leads to weak policy implementation, even when policies are already in place.

Not only lecturers, but students also need adequate digital literacy to be able to understand privacy risks, ethical use, and responsible ways of interacting with generative AI. According to Savandha & Pramesti (2025), students with low digital literacy are more prone to unethical behavior in the use of technology, including in the context of AI-based plagiarism and assessment result manipulation. Higher education institutions must ensure that AI literacy is part of the curriculum, not just as supporting material, but as a key competency required in the era of digital education.

The governance of generative AI in higher education also requires continuous monitoring and evaluation mechanisms. The use of AI is not static; generative models are constantly being updated, usage patterns are changing, and new risks are emerging as technology evolves. Therefore, universities need a technology ethics committee or special unit responsible for monitoring and evaluating AI use, as recommended by UNESCO (2023). This committee can serve to review internal policies, conduct periodic audits of AI use, develop usage guidelines based on regulatory developments, and ensure that AI use is in line with the academic mission and digital rights of students.

In the context of higher education in Indonesia, the governance of generative AI faces considerable structural challenges. Many universities do not yet have comprehensive data security policies, even though the implementation of the Personal Data Protection Law has become a national obligation. Another issue is the academic culture, which tends to be slow in responding to technological changes. As generative AI develops rapidly, the policy response of universities tends to lag behind, causing a policy lag that increases the risk of technology misuse. Arista et al. (2024) emphasize that universities in Indonesia need to modernize their digital governance so as not to fall behind in managing new risks that arise in education.

Beyond policy and infrastructure, generative AI governance must also consider fairness and inclusivity. Generative models, as demonstrated by Nguyen (2025), often exhibit bias toward specific social groups. If universities implement generative AI without considering cultural representation, language variation, and the needs of students with special needs, the risk of academic injustice will increase. Therefore, AI policies need to integrate the principle of algorithmic fairness to ensure that the technology is used equally by all students.

Thus, the institutional readiness of higher education institutions plays a key role in ensuring that the implementation of generative AI is ethical, safe, and fair. Higher education institutions must move from short-term needs-based use to structured strategic governance. Policies on the use of generative AI must include ethical guidelines, data security standards, competency development for faculty and students, strengthening of digital infrastructure, and sustainable monitoring mechanisms. Without robust governance, the risks of technology misuse will outweigh its benefits, which could ultimately undermine academic quality and public trust in higher education institutions.

4. Conclusions and Suggestions

The results of the analysis show that the implementation of generative artificial intelligence in higher education environments brings significant pedagogical benefits, but at the same time poses major challenges related to academic integrity, data security, and institutional readiness. Ethically, the use of generative AI has the potential to blur the line between students' original work and algorithmic output, increasing the risk of undetectable plagiarism and reducing critical thinking skills if used uncontrollably. On the other hand, academic data security is a major issue because most commercial generative AI platforms have non-transparent data storage mechanisms, exposing student and faculty interactions to third parties.

P-ISSN: 0000-0000; E-ISSN: 3025-1990
Available : https://jurnalhafasy.com/index.php/msj DOI: https://doi.org/10.61942/msj.v3i4.482

The risks of data leakage, uncertainty regarding the use of data for model training, and the vulnerability of university IT security systems reinforce the urgency of stricter supervision of the use of this technology. From an institutional perspective, most universities do not yet have comprehensive governance of AI use.

The lack of ethical guidelines, insufficient AI literacy among lecturers, inadequate digital security infrastructure, and the absence of systematic monitoring mechanisms indicate that the implementation of generative AI in many universities is still reactive and not supported by strategic policies. Without a strong institutional framework, the use of generative AI has the potential to increase academic inequality, exacerbate the risk of algorithmic bias, and reduce the quality of learning evaluation.

Considering the overall findings, this study recommends that universities develop generative AI ethical guidelines that regulate the limits of use in the learning and assessment processes, improve AI literacy for lecturers and students, strengthen data security through internal protocols and the integration of digital security standards, and form a technology oversight unit or committee to ensure that AI is used ethically and safely. A comprehensive, ethics-based governance approach will help higher education institutions make optimal use of generative AI without compromising academic values and the protection of academic community data.

Bibliografy

Ahmed, Z., Shanto, S. S., Rime, M. H. K., Morol, M. K., Fahad, N., Hossen, M. J., & Abdullah-Al-Jubair, M. (2024). *The generative AI landscape in education: Mapping the terrain of opportunities, challenges and student perception*. IEEE Access.

Al Kautsar, N. G., Fauzan, M., Pratama, R. A., & Rakhmawati, N. A. (2024). *Analisis pengaruh artificial intelligence (AI) terhadap kinerja akademik mahasiswa Sistem Informasi ITS*. Etika Teknologi Informasi, 1–10.

An, Y., Yu, J. H., & James, S. (2025). *Investigating the higher education institutions' guidelines and policies regarding the use of generative AI in teaching, learning, research, and administration*. International Journal of Educational Technology in Higher Education, 22(1), 10.

APJII. (2023). Laporan Survei Internet Indonesia 2023. Asosiasi Penyelenggara Jasa Internet Indonesia

Arista, A., Shuib, L., & Ismail, M. A. (2024, November). *Systematic literature review and bibliometric analysis on ethical policies for generative artificial intelligence (GAI) in higher education institutions (HEIs)*. In *2024 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)* (pp. 454–459). IEEE.

Dabis, A., & Csáki, C. (2024). *AI and ethics: Investigating the first policy responses of higher education institutions to the challenge of generative AI*. Humanities and Social Sciences Communications, 11(1), 1–13.

Fatmadiwi, A., Hartoyo, A., & Erlina, E. (2025). *Kebijakan Artificial Intelligence (AI) dalam pembelajaran di perguruan tinggi*. Jurnal Alwatzikhoebillah, 11(1), 284–291.

Gallent Torres, C., Zapata-González, A., & Ortego-Hernando, J. L. (2023). *The impact of generative artificial intelligence in higher education: A focus on ethics and academic integrity*. RELIEVE, 29(2), 1–19.

García-López, I. M., & Trujillo-Liñán, L. (2025). *Generative Artificial Intelligence in education: Ethical challenges, regulatory frameworks and educational quality in a systematic review of the literature*. Frontiers in Education, 10, 1565938.

Jin, Y., Yan, L., Echeverria, V., Gašević, D., & Martinez-Maldonado, R. (2025). *Generative AI in higher education: A global perspective of institutional adoption policies and guidelines*. Computers and Education: Artificial Intelligence, 8, 100348.

Junaedi, R. A. (2025). *Strategi komunikasi pendidikan berbasis generative AI dalam membangun pembelajaran di perguruan tinggi*. Jurnal Inovasi Komunikasi, 1–7.

Kamil, I., Miranda, T., & Setiawan, A. R. (2025). *Pengaruh kecerdasan buatan terhadap mahasiswa di perguruan tinggi*. JEDBUS, 2(1), 33–41.

Kasman, R. A., & HB, A. M. (2025). *Peran dan tantangan kecerdasan buatan (AI) dalam pendidikan tinggi: Implementasi dan implikasi etis*. Jurnal Pendidikan dan Pembelajaran, 5(1), 24–33.

Maulana, M. Z. (2025). *Pendidikan Islam adaptif di era digital: Sinergi AI generatif dan learning analytics*. Insight: Islamic Education and Learning, 1(2), 80–88.

Marlin, K., Tantrisna, E., Mardikawati, B., Anggraini, R., & Susilawati, E. (2023). *Manfaat dan tantangan penggunaan AI ChatGPT dalam proses pendidikan etika dan kompetensi mahasiswa*. Innovative Journal Of Social Science Research, 3(6), 5192–5201.

Mayasari, N., Sastraatmadja, A. H. M., Suhara, A., Jauhar, N., Hasan, S., & Maqfirah, P. A. V. (2025). *Artificial intelligence dalam pendidikan: Metode, implementasi, dan evaluasi*. Penerbit Widina.

McDonald, N., Johri, A., Ali, A., & Collier, A. H. (2025). *Generative artificial intelligence in higher education: Evidence from an analysis of institutional policies and guidelines*. Computers in Human Behavior: Artificial Humans, 3, 100121.

Nguyen, K. V. (2025). *The use of generative AI tools in higher education: Ethical and pedagogical principles*. Journal of Academic Ethics, 1–21.

Nur, S. A. A., Noni, N. N., & Nur, M. S. (2025). *Peran kecerdasan buatan dalam digitalisasi pendidikan: Tinjauan sistematis*. Journal of Indonesian Scholars for Social Research, 5(1 Special Issues), 29–33.

OECD. (2021). AI and the Future of Skills. Organisation for Economic Co-operation and Development.

Olohunfunmi, I. A., & Khairuddin, A. Z. (2024, December). *Exploring ethical dilemmas of AI generative tools among higher education students: A systematic review*. In *InvENT 2024* (pp. 255–275). Atlantis Press.

Resky, M., & Suharyat, Y. (2024). *Analysis of AI technology utilization in Islamic education*. Procedia of Social Sciences and Humanities, 5, 132–140.

Savandha, S. D., & Pramesti, G. N. D. P. (2025). *DeepSeek AI dan disrupsi teknologi Tiongkok*. Co-Value Jurnal Ekonomi Koperasi dan Kewirausahaan, 15(10).

UNESCO. (2023). Guidance for the Ethical Use of Artificial Intelligence in Higher Education.

Wibowo, A. (2025). *Pengantar AI, big data dan ilmu data*. Penerbit Yayasan Prima Agus Teknik.