EGE SCHOLAR JOURNAL

EGE SCHOLAR JOURNAL

Ege Scholar Journal, Year: 2025, Volume: 2, Issue: 2, Pages : 107-115 ***Research Article***

DOI: 10.5281/zenodo.18525373

Publication Date: 30.05.2025

Edmond Hajrizi[1]

1. UBT College (University for Business and Technology); Lagjja Kalabria, 10000 Prishtinë, Kosovë; edmond.hajrizi@ubt-uni.net; ORCID: 0000-0003-2883-8860

AI Policies in Higher Education: Risk Management, Academic Integrity, and EU AI Act Alignment for Partner Institutions

Abstract

Artificial intelligence (AI) is being adopted across higher education for advising, learning analytics, admissions triage, assessment support, and administrative efficiency. This diffusion creates measurable benefits but also introduces integrity risks (unauthorized assistance and undetected contract cheating), rights and privacy risks (profiling, surveillance, and automated decision-making), and safety/security risks (prompt injection, data exfiltration, and supply-chain vulnerabilities). This paper develops an implementable policy-and-compliance framework for partner institutions that integrates (i) institutional governance and role assignment, (ii) a use-case classification and risk-scoring rubric aligned with the EU AI Act's risk-based logic, (iii) academic integrity controls embedded in assessment design and disclosure rules, and (iv) monitoring, documentation, and auditability requirements grounded in recognized risk-management standards. An illustrative dataset scores six common university AI use cases on overall risk and academic integrity impact, demonstrating that proctoring and automated grading concentrate the highest risk, while advisory chatbots and research summarization are lower-risk but still require privacy and transparency controls. The paper concludes with a practical checklist and forward-looking scenarios (2027–2030) showing how governance maturity can reduce measured risk while compliance obligations and threat environments evolve.

Keywords: higher education; AI policy; academic integrity; risk management; compliance; governance; EU AI Act

How to cite: Hajrizi E. (2025).AI Policies in Higher Education: Risk Management, Academic Integrity, and EU AI Act Alignment for Partner Institutions. *Ege Scholar Journal, 2*(2), 107-115

1. Introduction

Generative and predictive AI systems have rapidly moved from experimental campus pilots to operational tools in advising, student support, learning analytics, assessment workflows, and institutional administration. Student uptake is now near-universal in some contexts; for example, the Higher Education Policy Institute (HEPI) and Kortext survey of UK undergraduates reported that 92% of students used AI in some form in 2025, up from 66% in 2024, and 88% reported using generative AI in assessments. Such diffusion changes the integrity baseline for universities: the question is no longer whether students will have access to AI assistance, but whether institutions can design credible, fair, and auditable learning and assessment systems under widespread AI use.At the same time, institutional AI adoption has moved into strategic planning. The 2025 EDUCAUSE AI Landscape Study (surveyed in November 2024) reports that 57% of higher-education respondents view AI as a strategic priority, reflecting increasing investment and partner-driven adoption. As universities enter collaborations with external AI providers or cross-border partner institutions, a coherent governance and compliance approach becomes a prerequisite for reputational protection, procurement discipline, and student trust.Three categories of risk motivate the framework proposed here. First, academic integrity risk encompasses unauthorized generation of text/code, undue assistance on take-home assessments, and the erosion of attribution and authorship norms. Second, rights and privacy risk includes surveillance and profiling (e.g., proctoring), automated decisions with significant effects (e.g., admissions triage), and opaque inferences from student data. The European Data Protection Board's guidance on automated decision-making and profiling underscores the need for safeguards where decisions produce legal or similarly significant effects. Third, safety and security risk reflects an evolving threat landscape: adversarial prompting, data leakage through third-party tools, and model supply-chain vulnerabilities.Policy design is further shaped by regulatory alignment. The EU Artificial Intelligence Act was published in the Official Journal in July 2024 and applies a risk-based structure, with a general date of application of 2 August 2026 and full effectiveness expected by 2027 as complementary standards and guidance mature. Partner institutions in EU-aligned environments therefore need a practical translation of 'risk-based compliance' into university procurement, governance, and assessment operations.This paper addresses the following research objective: to develop an implementable governance and risk-management framework for higher education institutions that (i) classifies AI use cases, (ii) quantifies risk and academic-integrity impact using auditable criteria, and (iii) specifies controls, documentation, and monitoring requirements aligned with the EU AI Act logic and recognized risk-management standards (e.g., NIST AI RMF and ISO/IEC 23894). The contribution is a policy blueprint and a measurement approach that can be used for partner due diligence, internal policy formation, and continuous improvement.

2. Materials and Methods

2.1. Framework design and source selection

The study applies a structured policy-synthesis and measurement design method. Normative and technical sources were selected to cover: (i) AI governance and risk management (NIST AI Risk Management Framework 1.0; ISO/IEC 23894:2023), (ii) higher-education integrity governance (academic integrity literature and practical controls), (iii) data protection and automated decision-making safeguards (EDPB guidance), (iv) cybersecurity threat context (ENISA Threat Landscape 2024), and (v) EU AI Act alignment and implementation timing.

2.2. Use-case catalogue and classification

Six representative AI use cases common to higher education were defined: automated grading, admissions triage, proctoring, learning analytics, chatbot advising, and research summarization. The set was chosen to span a spectrum of: (a) decision stakes, (b) automation level, (c) data sensitivity and subject vulnerability, and (d) susceptibility to misuse.

2.3. Risk scoring rubric

For each use case, two scores were computed on a 0–100 scale: (i) an overall RiskScore capturing rights, privacy, safety, and institutional risk, and (ii) an AcademicIntegrityImpact score capturing probability and severity of integrity compromise. Scores are derived from a rubric with five weighted dimensions: (1) stakes/impact of the decision or intervention; (2) automation level and degree of human oversight; (3) explainability and contestability; (4) data sensitivity and exposure risk; and (5) misuse potential (including plagiarism, impersonation, and coercive or surveillance applications). The rubric is designed to be auditable: institutions can document the basis for each rating, including tool capabilities, data flows, and control coverage.

2.4. Scenario logic for present–future comparisons

To satisfy the need for forward-looking policy planning, illustrative projections (2027 and 2030) were produced by applying governance-maturity adjustments to baseline scores. The adjustment represents the expected risk reduction from implementation of minimum viable controls: role assignment, documented use-case approval, privacy-by-design, security controls, transparency to students, and integrity-aligned assessment redesign. These projections are not causal estimates; they provide a structured way to compare ‘current state’ and ‘target state’ risk profiles for strategic planning.

3. Results

Table 1 reports baseline (current-state) scores for six AI use cases. The results concentrate the highest combined risk in proctoring and automated grading, consistent with their higher stakes, surveillance characteristics, and potential for contested outcomes. Advisory chatbots and research summarization exhibit lower direct-stakes risk but still require governance due to privacy exposure, hallucination risk, and potential misuse. Figure 1 visualizes the relationship between overall risk and integrity impact.To support ‘present versus future’ comparisons, Table 2 and Figure 2 provide an illustrative projection of risk scores for 2027 and 2030 under increasing governance maturity and alignment with emerging EU AI Act obligations and supporting standards. The projections show that risk reduction is feasible but bounded: high-stakes use cases remain high-risk even after controls, implying that institutions should either avoid them, restrict them to tightly governed contexts, or implement strong human oversight and contestability.

3.2. Figures, Tables and Schemes

Figure 1. Risk vs academic integrity impact across common higher-education AI use cases.

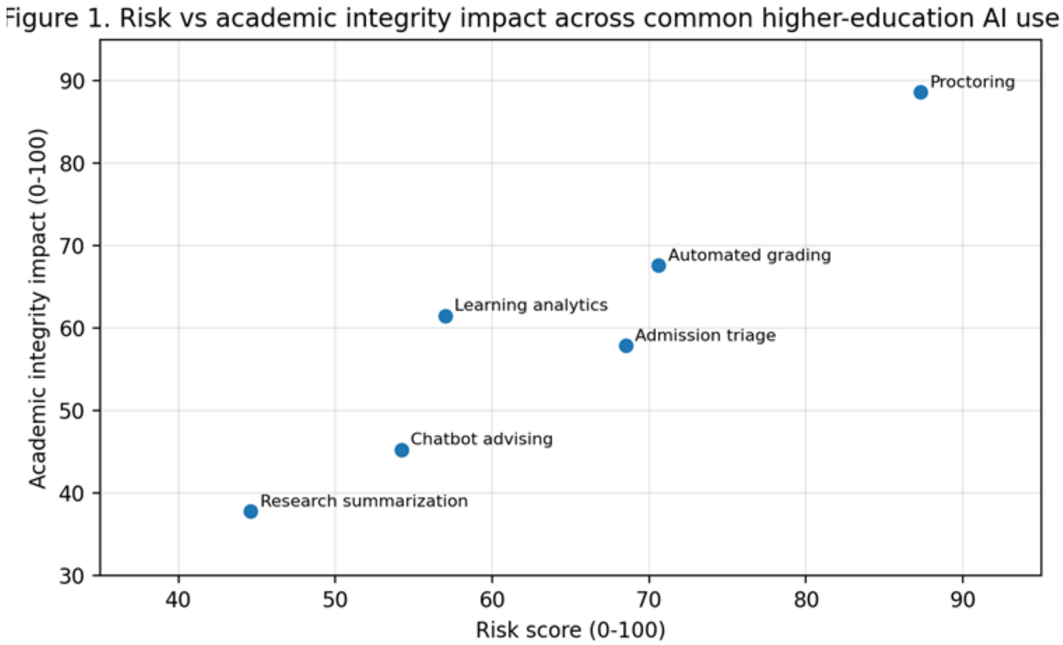


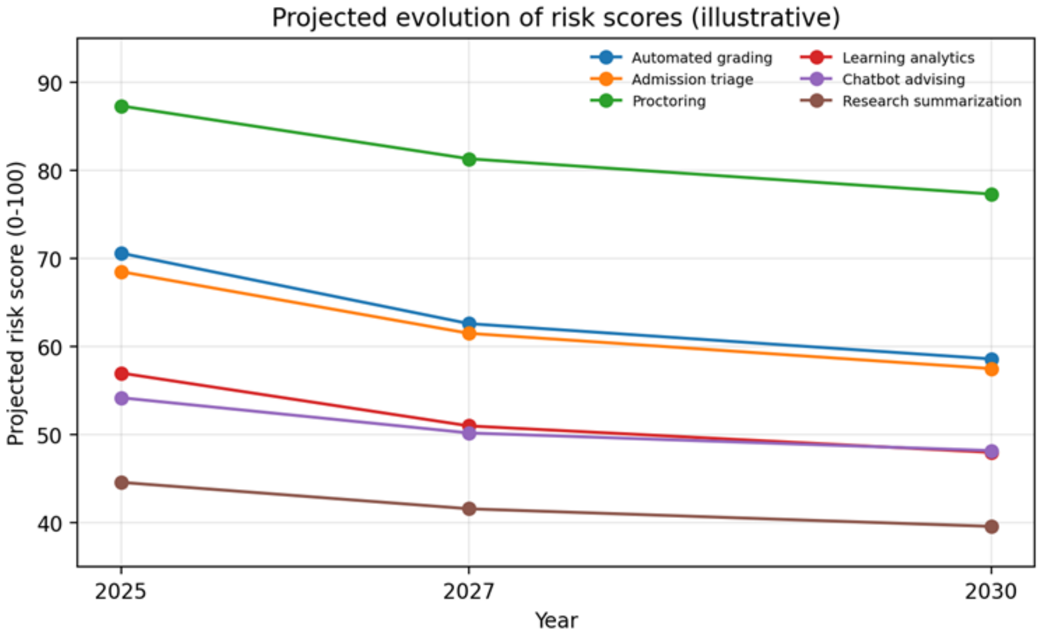
Table 1. Structured dataset used in this study (baseline scores).

HigherEd_AI_UseCase	RiskScore_0_100	AcademicIntegrityImpact_0_100
Automated grading	70.6	67.6
Admission triage	68.5	57.9
Proctoring	87.3	88.6
Learning analytics	57.0	61.5
Chatbot advising	54.2	45.3
Research summarization	44.6	37.8

Table 2. Illustrative present–future comparison of projected risk scores under governance maturity (2025–2030).

Use case	2025	2027	2030
Automated grading	70.6	62.6	58.6
Admission triage	68.5	61.5	57.5
Proctoring	87.3	81.3	77.3
Learning analytics	57.0	51.0	48.0
Chatbot advising	54.2	50.2	48.2
Research summarization	44.6	41.6	39.6

Figure 2. Projected evolution of risk scores under increasing governance maturity (illustrative).



4. Discussion

The results support three policy implications.

First, universities should treat proctoring and automated grading as high-risk deployments that require exceptional justification, strict data protection controls, and strong contestability. Proctoring concentrates surveillance and biometric-like inference risks, while automated grading can affect progression and fairness if models are not transparent, calibrated, and subject to human review. A 'default-to-human' principle is therefore defensible for consequential grading decisions, using AI primarily for low-stakes feedback and consistency checks rather than final determinations.Second, integrity governance should be embedded in assessment design rather than relying exclusively on detection. Evidence from student surveys indicates that AI use in assessments is widespread and rising. This pushes institutions toward redesign patterns that are robust to AI assistance: authentic assessments, oral defenses, staged drafts with process evidence, in-class performance components, and explicit disclosure requirements. UNESCO's guidance on generative AI in education and research emphasizes privacy protection and age-appropriate, human-centred use, which can be translated into institutional rules on tool selection, data minimization, and permitted pedagogical use.Third, compliance alignment is becoming an operational requirement for partner institutions. The EU AI Act's risk-based approach and implementation timeline implies that institutions should prepare well ahead of 2 August 2026 by creating a documented governance process: cataloguing AI systems, classifying use cases, ensuring supplier transparency, and establishing audit trails for training data provenance (where available), model documentation, and performance monitoring. The EDPB guidance on automated decision-making strengthens the case for procedural safeguards where AI contributes to admissions, scholarship decisions, or disciplinary outcomes.From an information security standpoint, the ENISA Threat Landscape highlights persistent availability, ransomware, and data-related threats. University AI policies should therefore be coupled with institution-wide security management practices (e.g., ISO/IEC 27001-aligned controls), including vendor risk assessment, access control, incident response procedures, and continuous monitoring.Limitations are deliberate: the dataset is an illustrative scoring exercise, not an empirical causal study. However, the approach is still decision-useful: it supports consistent triage, documentation, and prioritization of controls, and it provides a quantitative baseline against which institutions can measure improvements over time.

5. Conclusions

This paper provides a practical governance and compliance framework for higher education institutions adopting AI in partnership contexts. By combining a use-case catalogue, a transparent risk-scoring rubric, and integrity controls embedded in assessment and disclosure rules, institutions can move from ad hoc AI adoption to defensible, auditable governance. The results indicate that high-stakes deployments (notably proctoring and automated grading) remain high-risk even under strengthened governance, while lower-stakes applications (chatbot advising and research summarization) can be adopted more safely with privacy-by-design, transparency, and monitoring.Forward-looking comparisons (2027–2030) illustrate that governance maturity can reduce measured risk, but only if institutions invest in role assignment, documentation, supplier due diligence, and continuous evaluation. Future research should validate the rubric against observed outcomes: integrity incidents, appeals, student trust metrics, and documented privacy/security events. Such validation would enable more precise calibration of risk scores and support evidence-based sector benchmarking.

6. Patents

Not applicable.

Supplementary Materials

The structured datasets (Table 1) and scenario projections (Table 2) are available as machine-readable CSV files. Institutions may adapt the rubric weights and add local use cases (e.g., library search assistants, accessibility tools, or AI-supported tutoring).

Author Contributions

Conceptualization, E.H.; methodology, E.H.; formal analysis, E.H.; writing—original draft preparation, E.H.; writing—review and editing, E.H.; visualization, E.H.; supervision, E.H. All authors have read and agreed to the published version of the manuscript.

Funding

This research received no external funding.

Institutional Review Board Statement

Not applicable. This study relies on public sources and does not involve human subjects research.

Informed Consent Statement

Not applicable.

Acknowledgments

The author acknowledges institutional discussions on responsible AI adoption and academic integrity in higher education.

Conflicts of Interest

The author declares no conflicts of interest.

Appendix A

- Minimum Viable AI Governance Checklist for Partner Institutions Approved AI policy with roles (owner, DPO, security lead, academic integrity lead).
- Use-case register and risk classification (including high-stakes/high-risk flag).
- Assessment integrity controls (disclosure rules, authentic assessments, oral verification).
- Data protection impact assessment where required; data minimization and retention rules.
- Supplier due diligence and contractual clauses (security, logging, deletion, transparency).
- Monitoring and incident response (misuse reporting, security events, appeals process).
- Annual review and re-scoring of use cases.

Appendix B

Data dictionary

RiskScore_0_100: Composite score for rights, privacy, safety, and institutional risk (0=low, 100=high).

AcademicIntegrityImpact_0_100: Composite score for integrity harm likelihood and severity (0=low, 100=high).

Projected scores (2027, 2030): Illustrative ‘target-state’ scores after governance maturity improvements.

References

1. European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union.

2. European Parliamentary Research Service. (2025). AI Act implementation timeline (PE 772.906). European Parliament.

3. UNESCO. (2023). Guidance for generative AI in education and research. UNESCO.

4. National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce.

5. ISO/IEC. (2023). ISO/IEC 23894:2023 Information technology—Artificial intelligence—Guidance on risk management. International Organization for Standardization.

6. ISO/IEC. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements. International Organization for Standardization.

7. European Data Protection Board. (2018). Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251 rev.01). EDPB.

8. European Commission. (2020). Digital Education Action Plan 2021–2027: Resetting education and training for the digital age. European Commission.

9. ENISA. (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity.

10. OECD. (2019). OECD principles on artificial intelligence. OECD Publishing.

11. European Commission. (2022). Ethics guidelines for trustworthy AI. European Commission.
12. Council of Europe. (2020). Guidelines on AI and data protection in education. Council of Europe.
13. Selwyn, N. (2019). Should robots replace teachers? Polity Press.
14. Williamson, B., Eynon, R., & Potter, J. (2020). Pandemic politics, pedagogies and practices: Digital technologies and distance education. Learning, Media and Technology, 45(2), 107–114.
15. Zawacki-Richter, O., Marín, V. I., Bond, M., & Gouverneur, F. (2019). Systematic review of research on artificial intelligence applications in higher education. International Journal of Educational Technology in Higher Education, 16(1), 39.
16. Holmes, W., Bialik, M., & Fadel, C. (2019). Artificial intelligence in education. Center for Curriculum Redesign.
17. Luckin, R. (2018). Machine learning and human intelligence. UCL IOE Press.
18. Bretag, T. (Ed.). (2016). Handbook of academic integrity. Springer.
19. Eaton, S. E. (2021). Plagiarism in higher education: Tackling tough topics in academic integrity. Springer.
20. Sutherland-Smith, W. (2008). Plagiarism, the internet, and student learning. Routledge.
21. IEEE. (2019). Ethically aligned design: A vision for prioritizing human well-being with autonomous and intelligent systems. IEEE.
22. Shneiderman, B. (2020). Human-centered AI. Oxford University Press.
23. Floridi, L. (2019). Establishing the rules for building trustworthy AI. Nature Machine Intelligence, 1, 261–262.
24. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. International Data Privacy Law, 7(2), 76–99.
25. Slade, S., & Prinsloo, P. (2013). Learning analytics: Ethical issues and dilemmas. American Behavioral Scientist, 57(10), 1510–1529.
26. Baker, R. S. (2019). Challenges for the future of educational data mining: The Baker learning analytics prizes. Journal of Educational Data Mining, 11(1), 1–17.
27. Kizilcec, R. F., & Lee, H. (2020). Algorithmic fairness in education. arXiv:2007.07053.
28. Murtezaj, I. M., Rexhepi, B. R., Xhaferi, B. S., Xhafa, H., & Xhaferi, S. (2024). The study and application of moral principles and values in the fields of accounting and auditing. Pakistan Journal of Life and Social Sciences, 22(2), 3885–3902. https://doi.org/10.57239/PJLSS-2024-22.2.00286
29. Murtezaj, I. M., Rexhepi, B. R., Dauti, B., & Xhafa, H. (2024). Mitigating economic losses and prospects for the development of the energy sector in the Republic of Kosovo. Economics of Development, 23(3), 82–92. https://doi.org/10.57111/econ/3.2024.82
30. Rexhepi, B. R., Murtezaj, I. M., Xhaferi, B. S., Raimi, N., Xhafa, H., & Xhaferi, S. (2024). Investment decisions related to the allocation of capital. Educational Administration: Theory and Practice, 30(6), 513–527. https://doi.org/10.53555/kuey.v30i6.5233

31. Rexhepi, B. R., Murtezaj, I. M., Xhaferi, B. S., Xhafa, H., & Xhaferi, S. (2024). Tax accounting in the Republic of Kosovo. Educational Administration: Theory and Practice, 30(6), 529–535. https://doi.org/10.53555/kuey.v30i6.5245

32. Rexhepi, B. R., Rexhepii, F. G., Xhaferi, B., Xhaferi, S., & Berisha, B. I. (2024). Financial accounting management: A case of Ege Furniture in Kosovo. Quality-Access to Success, 25(200). https://doi.org/10.47750/QAS/25.200.09