Digital Governance of Learning Data in Public Education Initiatives

Authors

Mikkel Sørensen[1], Freja Madsen[2*], Anders Kristensen[3]

Affiliations

Department of Computer Science, Faculty of Science, University of Copenhagen, Universitetsparken 1, DK-2100 Copenhagen Ø, Denmark.

***Corresponding author:** freja.madsen@di.ku.dk

Abstract

This study develops a digital governance framework for managing learning data in public education initiatives. The study is designed to examine approximately 60 public education programs using digital attendance systems, online learning platforms, learner profiles, automated assessment tools, and feedback databases. Data are collected from institutional policy documents, platform-use records, administrator surveys, learner consent forms, privacy notices, access-control logs, and user trust questionnaires. The dataset is expected to include around 60 governance policy files, 300 administrator responses, 2,000 learner questionnaires, 500 consent records, and 120,000 anonymized access-control logs. The study measures data ownership clarity, consent transparency, privacy protection, access-control strength, data-use explainability, retention policy completeness, breach-response readiness, and learner trust. Quantitative analysis applies governance maturity scoring, factor analysis, cluster analysis, logistic regression, and structural equation modeling to examine how data governance quality affects learner trust and institutional credibility. The study also identifies different governance maturity types, such as compliance-oriented, platform-dependent, risk-reactive, and transparency-driven models. The innovation of this study lies in connecting educational data governance with measurable learner trust and institutional accountability, providing a practical evaluation model for public education programs that increasingly rely on digital learning records and automated decision-support systems.

Keywords: learning data governance; public education; data privacy; access control; learner trust; governance maturity; educational technology; institutional accountability

1. Introduction

Public education programs increasingly rely on digital systems to organize teaching, participation, assessment, and learner support. Digital attendance systems, learning management platforms, online assessments, learner profiles, communication tools, and feedback databases are now embedded in many educational settings. Their use has also expanded beyond conventional schools and universities to public libraries, cultural centers, community colleges, arts education programs, and other publicly supported learning services. In public art education, for example, recent research has examined how collaborative teaching models and the organization of teaching resources can be improved through more systematic and efficient resource coordination [1]. Such developments reflect a broader shift toward data-supported educational management, in which digital platforms are not only used to deliver learning activities but also to allocate resources, monitor participation, evaluate performance, and support administrative decision-making. As these functions become increasingly interconnected, educational institutions accumulate large volumes of information concerning learner identity, attendance, academic performance, learning behavior, communication, platform activity, and service use. These data can improve instructional coordination and institutional efficiency, but they also create governance questions concerning who owns the data, who is permitted to access them, how long they should be retained, whether learners understand the purposes of collection, and how automated or data-based decisions should be explained. Learning data governance therefore extends beyond conventional cybersecurity or technical data protection. It concerns the institutional rules and operational procedures through which educational data are collected, classified, accessed, shared, retained, interpreted, and deleted. Effective governance requires attention to privacy protection, data quality, staff responsibilities, third-party services, retention periods, access authorization, consent procedures, accountability mechanisms, and explanations provided to learners. Existing research indicates that privacy is still inconsistently defined across learning analytics studies, making it difficult to translate broad ethical principles into routine institutional practice [2,3]. Privacy also cannot be considered independently of trust and personalization because learners may evaluate the acceptability of data collection partly according to the educational value they expect to receive from data-driven services [4]. Consent presents a related challenge. Learners may formally authorize data collection while having only a limited understanding of what information is collected, how long it is stored, what secondary purposes it may serve, and which organizations may eventually receive it. Institutional trust, perceived benefits, and concerns about the volume of collected data can substantially influence consent decisions [5,6]. Learners also tend to be more willing to provide information directly to educational institutions than to commercial organizations, while concern often increases when educational data are transferred to external service providers [7]. These findings suggest that formal consent alone cannot demonstrate meaningful learner control. Transparent governance requires institutions to communicate data purposes, access conditions, withdrawal procedures, sharing arrangements, and possible future uses in language that learners can reasonably understand.

Trust has consequently become an important outcome of educational data governance rather than merely a general attitude toward technology. Learners may be more willing to accept institutional data use when they perceive the institution as competent, fair, transparent, and accountable. Evidence suggests that students may tolerate a certain degree of privacy loss when they expect clear educational benefits, but this acceptance remains closely connected to the availability of understandable information about how their data are being used [8]. Privacy expectations also vary across countries, institutional cultures, and social contexts, indicating that governance arrangements cannot always be transferred directly from one setting to another [9,10]. Similar differences can be found among educational professionals. Teachers and administrators may place greater confidence in internal institutional systems than in external vendors, particularly when responsibilities for data ownership, data quality, access authorization, and platform management are unclear [11]. The rapid adoption of artificial intelligence in education further increases the importance of this issue because trust in AI-based educational tools depends not only on their technical performance but also on perceptions of transparency, institutional responsibility, and appropriate data use [12]. In this sense, learner trust is shaped by observable governance practices as well as by the technological functions of the system itself. Current governance frameworks commonly emphasize transparency, privacy, fairness, accountability, safety, and meaningful human oversight as central principles for responsible educational technology [13,14]. Human-centered approaches additionally argue that learners and teachers should participate more actively in the design, evaluation, and oversight of data-intensive educational systems [15]. However, the practical implementation of these principles remains uneven. Many institutions publish privacy statements or data-use policies, yet written policies do not necessarily reveal whether access permissions are appropriately restricted, whether obsolete records are actually deleted, whether staff access is routinely reviewed, or whether procedures exist for responding to misuse and security incidents. Audit-based approaches have therefore been proposed to examine system objectives, datasets, risks, organizational responsibilities, and post-deployment monitoring in a more structured manner [16,17]. Privacy-by-design approaches may further reduce unnecessary data centralization and restrict access to information that is not essential for educational purposes [18,19]. These developments indicate a gradual shift from principle-based discussions toward operational governance, but empirical studies linking policy requirements to observable institutional practices remain limited.

A major limitation of the existing literature is the separation between perceived governance and actual governance. Much of the evidence on privacy, consent, and trust is derived from questionnaires, interviews, or stated preferences. Such data are useful for understanding learner attitudes but provide limited information about how educational institutions actually manage data in daily operations [20]. For example, a learner may report high trust in an institution even though access permissions are excessively broad, retention periods are undefined, or consent records are incomplete. Conversely, an institution may have relatively strong technical controls while failing to communicate them clearly, resulting in low learner confidence. Access-control logs, retention schedules, consent records, privacy notices, data-sharing rules, and breach-response procedures are rarely analyzed together with learner perceptions. As a result, there remains a substantial gap between research on the ethical principles of educational data use and research on the measurable institutional practices through which those principles are implemented. This gap is particularly important in public education programs. Compared with large universities, smaller public education providers may have fewer specialized data-management staff, greater dependence on third-party platforms, and more heterogeneous learner populations. They may also operate across different instructional contexts, including non-degree education, community learning, public arts programs, adult education, and cultural services. Governance practices in such settings can therefore differ considerably even when institutions use similar digital platforms. Research conducted in China has identified related problems, including unclear institutional responsibilities, incomplete governance standards, difficult-to-understand privacy notices, and uncertainty concerning secondary data use and reuse [21,22]. Nevertheless, existing studies remain concentrated on universities, formal online-learning environments, or individual platforms. Public libraries, cultural centers, community colleges, public arts programs, and other local education services have received substantially less systematic attention. This leaves limited evidence regarding how governance quality varies across public education programs, whether common governance patterns can be identified, and which institutional practices are most strongly associated with learner trust [23,24]. Another unresolved issue concerns governance maturity. Privacy protection, consent transparency, access control, data-use explanation, retention management, and breach response are often examined as separate variables, although they operate as interdependent components of an institutional governance system. Strong performance in one area does not necessarily indicate strong overall governance. An institution may provide detailed privacy notices while maintaining weak access controls, or it may implement technically restrictive access permissions without explaining data practices adequately to learners. Governance quality is therefore better understood as a multidimensional institutional capability rather than a single compliance indicator. Existing research has rarely classified education programs according to combinations of governance practices or examined whether distinct governance profiles emerge across institutions. A maturity-based perspective can help distinguish organizations that primarily emphasize formal compliance from those that rely heavily on technology providers, respond mainly after risks arise, or embed transparency and accountability more consistently into routine practice. Such a classification may provide a more useful basis for institutional comparison and improvement than isolated measurements of individual privacy or security practices.

Accordingly, this study aims to develop and empirically evaluate a multidimensional framework for assessing learning data governance in public education programs and to examine how differences in governance practice are associated with learner trust and institutional credibility. Approximately 60 public education programs using digital learning systems are examined by integrating 60 policy files, 300 administrator surveys, 2,000 learner questionnaires, 500 consent records, and approximately 120,000 anonymized access-control logs. The analysis evaluates data ownership clarity, consent transparency, privacy protection, access-control strength, data-use explanation, retention-policy completeness, breach-response readiness, and learner trust. Factor analysis is used to examine the underlying structure of the governance measures, while governance maturity scoring evaluates the overall level and balance of institutional practices. Cluster analysis is employed to identify recurring governance profiles, including compliance-oriented, platform-dependent, risk-reactive, and transparency-driven programs. Logistic regression and structural equation modeling are further used to examine the relationships among governance quality, learner trust, and institutional credibility. By combining policy documents, administrative information, consent records, system-level behavioral evidence, and learner perceptions within the same analytical framework, the study moves beyond evaluations based solely on stated policies or self-reported attitudes. Its significance lies in providing an operational method for determining whether governance principles are reflected in actual institutional practice, identifying weaknesses that may remain hidden behind formal compliance, and offering public education providers a measurable basis for improving consent procedures, access management, transparency, retention practices, and accountability. The resulting framework can also support more consistent governance standards for increasingly data-intensive public learning environments while helping institutions balance the educational value of digital systems with the protection of learner rights and long-term institutional trust.

2. Materials and Methods

2.1 Sample and Study Setting

The study included 60 public education programs from community colleges, public libraries, cultural centers, adult learning institutes, and local training agencies in four urban areas. Each program used at least three digital systems, such as electronic attendance tools, online learning platforms, learner databases, automated assessment tools, or feedback systems. Programs were included when they had operated for at least one year, stored learner data in digital form, and had written privacy or data-use rules. Programs with incomplete access logs or missing consent records were excluded. The dataset included 60 governance policy files, 300 administrator surveys, 2,000 learner questionnaires, 500 consent records, and about 120,000 anonymous access logs. Administrator data included job role, years of service, data duties, and training history. Learner data included age group, education level, program type, digital experience, and prior use of online learning systems.

2.2 Study Design and Comparison Groups

A matched quasi-experimental design was used. Thirty programs formed the governance-support group, and 30 formed the comparison group. Programs were matched by institution type, learner number, delivery mode, number of digital systems, and baseline privacy score. The governance-support group used a standard checklist for one semester. The checklist covered data ownership, consent, access rights, storage time, data-use explanation, deletion rules, and breach response. Staff also received two hours of training and a plain-language privacy notice for learners. The comparison group continued its usual data-management practice. Both groups used the same teaching systems and course procedures. Data were collected before and after the intervention. This design tested whether clearer governance rules improved learner trust and reporting quality without changing course content.

2.3 Measures and Quality Control

Governance quality was measured in seven areas: ownership clarity, consent transparency, privacy protection, access-control strength, data-use explanation, retention policy completeness, and breach-response readiness. Each area contained four to six items scored on a five-point scale. Learner trust covered confidence in data security, fairness, institutional honesty, control over personal data, and willingness to continue using digital services. Institutional credibility covered perceived competence, responsibility, and openness. Policy scores were checked against consent forms, privacy notices, and system records. Access-control strength was measured through failed login attempts, inactive accounts, repeated access, role conflicts, and access outside normal working hours. Two researchers reviewed 20% of the policy files and consent records independently. Cohen's kappa values above 0.75 were accepted. Cronbach's alpha was used to test survey consistency, and values above 0.70 were required. A pilot study with five programs, 25 administrators, and 120 learners was used to revise unclear items.

2.4 Data Processing and Model Formulas

The data were checked for duplicate records, missing values, extreme responses, and date errors. Missing values below 5% were estimated by multiple imputation. Variables measured on different scales were standardized before analysis. Exploratory and confirmatory factor analyses were used to test the structure of the governance measures. The governance maturity score for program i was calculated as:

$$GMS_i = \sum_{j=1}^{m} w_j z_{ij}$$

where z_{ij} is the standardized score of program i for governance area j, w_j is the factor-based weight, and mmm is the number of governance areas. Logistic regression was used to estimate the probability of high learner trust:

$$P(T_i=1) = \frac{1}{1+\exp\left[-(\beta_0+\beta_1 G_i+\beta_2 C_i+\beta_3 A_i+\beta_4 X_i)\right]}$$

where $T_i=1$ indicates high trust, G_i is governance quality, C_i is consent clarity, A_i is access-control strength, and X_i includes learner and program control variables. Cluster analysis was used to identify common governance types. Structural equation modeling was used to test the links among governance quality, transparency, learner trust, and institutional credibility.

2.5 Model Testing and Ethical Procedures

Group differences were tested before and after the intervention. Difference-in-differences analysis was used to estimate the effects of the governance checklist and staff training. Cluster quality was tested with silhouette scores and repeated sampling. Model fit was assessed with CFI, TLI, RMSEA, and SRMR. Results were also compared across institution types, delivery modes, and learner groups. Access logs were anonymized before transfer. Names, account numbers, and device identifiers were removed. Learners and administrators received study information and gave informed consent. Participation was voluntary, and withdrawal had no effect on course access or employment. Personal data were not used for grading, discipline, or service denial. All files were stored on an encrypted server and were available only to the research team.

3. Results and Discussion

3.1 Governance Maturity and Program Types

All 60 programs were included after data screening. The final dataset contained 296 administrator responses, 1,946 learner questionnaires, 487 consent records, and 118,436 valid access-log entries. Factor analysis supported the seven-part governance structure. The seven dimensions explained 73.8% of the total variance, and Cronbach's alpha was 0.89. The mean governance maturity score was 0.58, with values ranging from 0.29 to 0.84. Access-control strength had the highest mean score of 0.69, followed by privacy protection at 0.64 and data ownership clarity at 0.61. Lower scores were found for consent transparency at 0.52, retention policy completeness at 0.48, and breach-response readiness at 0.44. Cluster analysis identified four program types: compliance-oriented programs (n = 19), transparency-driven programs (n = 16), platform-dependent programs (n = 14), and risk-reactive programs (n = 11). Transparency-driven programs had the highest learner trust score, while risk-reactive programs had the lowest score (Fig. 1). These results show that technical controls were more common than clear consent rules, deletion policies, and breach-response plans [25,26]. Du et al. (2025) also reported a shift from separate departmental control toward more open data governance. However, many programs in the present study had not reached this stage. Gilbert et al. (2025) found that learners valued transparency but often had limited knowledge of data governance. The present study adds evidence from policy files, access logs, and learner surveys.

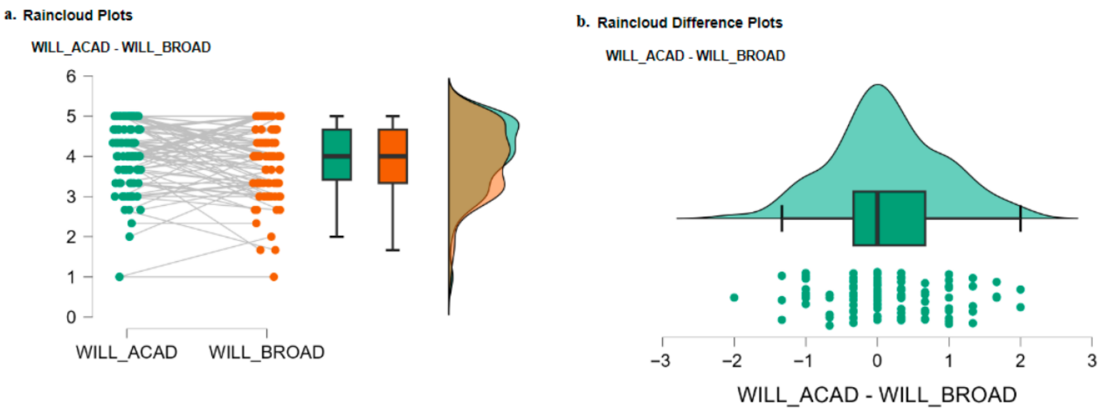

Fig. 2. Links among governance quality, transparency, learner trust, and institutional credibility.

3.2 Effects of Governance Support

The governance-support and comparison groups had similar baseline maturity scores of 0.51 and 0.50, respectively ($p = 0.73$). After one semester, the mean score increased to 0.71 in the governance-support group and to 0.55 in the comparison group. Difference-in-differences analysis showed a net increase of 0.15 points (95% CI = 0.10–0.20, $p < 0.001$). The largest gains were found in consent transparency (+0.24), retention policy completeness (+0.20), and breach-response readiness (+0.18). Access-control strength increased by 0.11 points, while data ownership clarity increased by 0.09 points. The number of inactive staff accounts with active permissions fell by 41.7%, and access events outside assigned roles fell by 34.5%. Learner trust increased from 3.18 to 3.82 in the governance-support group and from 3.20 to 3.34 in the comparison group. These findings show that a short checklist and staff training improved both written rules and daily practice. However, learner understanding improved more slowly. About 28% of learners in the governance-support group still did not know how long their data would be stored [27]. Tamana et al. (2026) found that institutional trust was closely related to willingness to allow educational data use. Learners also valued clear safeguards and limits on access. The present results support these findings and show that trust improves when institutions change their actual procedures rather than only revise privacy notices.

3.3 Relations Among Governance Quality Trust and Credibility

Logistic regression showed that governance maturity was the strongest predictor of high learner trust (OR = 2.45, 95% CI = 1.91–3.15, $p < 0.001$). Consent transparency (OR = 1.74, $p = 0.003$), access-control strength (OR = 1.59, $p = 0.011$), and clear explanations of data use (OR = 1.88, $p < 0.001$) also had positive effects. Retention rules were significant only when learners knew that the rules existed (OR = 1.42, $p = 0.038$). A written policy alone did not increase trust. The structural model showed acceptable fit, with CFI = 0.956, TLI = 0.948, RMSEA = 0.045, and SRMR = 0.040. Governance quality had a direct effect on transparency ($\beta = 0.48$, $p < 0.001$) and a smaller direct effect on learner trust ($\beta = 0.24$, $p = 0.006$). Transparency had a stronger effect on trust ($\beta = 0.41$, $p < 0.001$), while trust was closely related to institutional credibility ($\beta = 0.52$, $p < 0.001$). The indirect effect of governance quality on institutional credibility through transparency and trust was 0.20 (95% CI = 0.14–0.28) (Fig. 2). These results show that internal controls do not build trust unless learners can see and understand them [28]. Yang et al. (2025) also found that formal governance had a weaker effect than institutional culture on legal and ethical awareness. The present study reaches a similar conclusion and extends it to learner trust and institutional credibility.

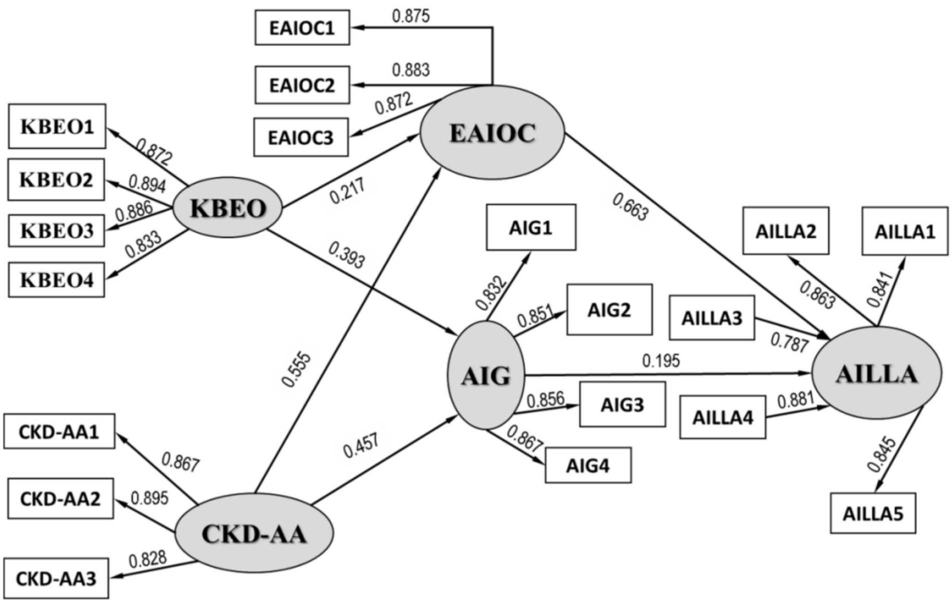

Fig. 2. Links among governance quality, transparency, learner trust, and institutional credibility.

3.4 Differences Across Programs and Practical Use

Governance quality differed by institution type and platform dependence. Community colleges had the highest mean maturity score of 0.68, followed by adult learning institutes at 0.61 and public libraries at 0.56. Cultural centers had the lowest score of 0.49. Programs that managed their own learner databases had clearer ownership and retention rules than programs that relied mainly on outside platforms. Platform-dependent programs recorded an average of 2.7 unresolved role conflicts per 1,000 access events, compared with 1.1 in transparency-driven programs. Learners in programs with clear opt-out procedures reported higher trust than those who received only general consent notices (3.91 vs. 3.29, $p < 0.001$). Trust also differed by digital experience, but this effect was smaller than the effect of governance type [29,30]. zhang et al. (2026) found that privacy concerns differ across national and cultural settings, which suggests that one governance model may not suit every learner group. Myeong et al. (2026) also noted that weak user involvement can reduce trust in learning analytics. The present findings support the use of short privacy notices, clear retention periods, regular account checks, role-based access, and simple ways to withdraw consent. The study was limited to four urban areas and one semester of follow-up. Access logs recorded system actions but did not always explain why they occurred. Learner trust was also based on self-reported data. Future studies should include rural programs, longer follow-up periods, direct security audits, and different legal settings.

4. Conclusion

This study developed a digital governance framework for public education programs that use learning platforms, digital records, and automated tools. The results showed that stronger governance was linked to higher learner trust and greater institutional credibility. Clear consent rules, strong access control, simple explanations of data use, complete retention policies, and breach-response plans were the main factors that shaped governance quality. Programs that used the governance checklist and staff training had better policy compliance, fewer access conflicts, and higher trust scores than the comparison group. The main contribution of this study is that it combines policy files, learner surveys, administrator responses, consent records, and access logs in one evaluation model. This method helps reveal the gap between written rules and daily data practice. The framework can help public education providers improve privacy protection, consent procedures, data access, and storage rules. It can also support comparisons of governance maturity across different programs. However, the study included only 60 programs in four urban areas and covered one semester. Learner trust was based on self-reported data, and access logs could not fully explain the reason for each action. Future research should include more regions, longer study periods, rural programs, and direct security audits.

References

1. Lin, T., Chen, A., & Spivack, Z. (2026). Research on Collaborative Piano Teaching Models and Teaching Resource Efficiency Optimization in Public Art Education Systems. Available at SSRN 6284818.
2. Malomo, O. O., Adekoya, A. A., Donald, A. M., Eyob, E., Omojokun, E., Mummalaneni, V., & Garuba, M. (2025). AI as asset and liability: A dual-use dilemma in higher education and the SPARKE Framework for institutional AI governance. Online Journal of Applied Knowledge Management (OJAKM), 13(2), 57-76.
3. Hong, Z., Xu, T., & Chen, H. (2026). Automated Detection and Reclamation of Orphaned Compute and Storage Resources in Cloud Infrastructure. Available at SSRN 7116258.
4. Alhazmi, A. K. (2026). Data Privacy and Security in AI-Driven Education Systems. In Revolutionizing Secure Learning in the Age of AI (pp. 263-294). IGI Global Scientific Publishing.
5. Rodriguez Müller, A. P., Tangi, L., & Lerusse, A. (2025). Understanding the adoption of artificial intelligence in local government decision-making: The influence of institutional pressures and managerial perceptions. Public Administration.
6. Li, J., Zhang, Y., & Gu, Y. (2026). Chain-Hash Audit Framework with Trusted Anchoring for Tamper-Evident Evidence Lifecycle Management.
7. Zhang, Y., Gu, W., & Wang, J. (2025, December). Research on First Article Inspection (FAI)-Driven Quality Assurance Methods for Wind Turbine Installation and Operation & Maintenance and Their Effect on Reliability Improvement. In Proceedings of the 2025 6th International Conference on Computer Science and Management Technology (pp. 1700-1705).
8. Huang, R. (2026). Edge-Centric Generative AI: A Survey on Efficient Inference for Large Language Models in Resource-Constrained Environments. Journal of Computer and Communications, 14(4), 238-253.

9. Da Costa, J., Cloke, H. L., Neumann, J., & Salvidge, N. (2025). Warning cultures in practice: shadow systems in local flood risk governance. Progress in Disaster Science, 100513.
10. Lin, T., Spivack, Z., & Chen, A. (2026). Monitoring Teaching Quality and Validating Educational Equity in Public Art Education. Available at SSRN 6512778.
11. Wu, J., Zhang, J., Wu, D., & Peng, Y. (2026). Visual Transformation Mechanisms for Integrating Digital Cultural Heritage Resources into Junior High School Art Curricula.
12. Alibayeva, R. N., & Allayarova, S. U. (2025). From data to pedagogy: leveraging explainable artificial intelligence to enhance trust, transparency, and effectiveness in intelligent learning systems. Qubahan Techno Journal, 4(3), 51-65.
13. Gui, H., Fu, Y., Wang, Z., & Zong, W. (2025). Research on Dynamic Balance Control of Ct Gantry Based on Multi-Body Dynamics Algorithm.
14. Wang, Y., Wang, Y., Yin, X., Arias, R., & Chen, J. (2026). Research on Dynamic Assessment of Glucose-Lipid Metabolism and Personalized Drug Response Prediction Based on Wearable Multimodal Sensing.
15. Ko, E. G., & Hughes, J. E. (2026). Value-Sensitive Design in Action: Designing Student-Centered Intelligent Tutoring Systems with Community College Students and Instructors. Computers and Education: Artificial Intelligence, 100560.
16. Zhang, Z., Tong, Y., & Gao, Y. (2026). Causal Representation Learning for Explainable Early Warning in High-Stakes Decision Systems.
17. Qi, C., & Qiao, X. (2026, May). Design Patterns for Multi-Agent Systems in Production. In 2026 International Conference on Intelligent Systems, Automation and Control (ISAC) (pp. 198-202). IEEE.
18. Ismail, I. A., & Aloshi, J. M. R. (2025). Data privacy in AI-driven education: An in-depth exploration into the data privacy concerns and potential solutions. In AI applications and strategies in teacher education (pp. 223-252). IGI Global Scientific Publishing.
19. Su, D., & Wu, Y. (2026). Multilevel Growth and Social Network Modeling for Functional Communication Enhancement in Students with Intellectual Disabilities.
20. Gao, G., Gao, R., Lu, C., Gao, R., & Kuang, Y. (2026, March). Security Governance Methods and Quantitative Evaluation for Enterprise SMS and Verification Code Systems. In 2026 International Conference on Generative Artificial Intelligence and Information Security (GAIIS) (pp. 455-458). IEEE.
21. Rüland, A. L., & Rüffin, N. (2026). Uncertainty and de facto policy design from below: the case of research security. Policy Design and Practice, 1-11.
22. Xiong, W., Guo, Y., & Zeng, Y. (2026). A Study on the Energy Efficiency of MEP Systems and Coordinated Dispatch Mechanisms for Multi-energy Systems in High-density Urban Buildings. Available at SSRN 7120518.

23. Bettahi, A., Beloudha, F. Z., & Harroud, H. (2025). Continuous-time modeling in educational data mining and learning analytics: a literature review on methods, ethics, and emerging AI trends. IEEE Access.
24. Hong, Z., Xu, T., & Chen, H. (2026). A Study on Test Coverage Mapping and Release Risk Prediction in Continuous Delivery of Cloud Services.
25. Du, Y. (2025). Research on Digital Quality Traceability System for Temperature-Controlled Supply Chain of Foreign Trade Wine Driven by Blockchain and IoT. Business and Social Sciences Proceedings, 4, 57-65.
26. Gilbert, C., & Gilbert, M. A. (2025). Impact of General Data Protection Regulation (GDPR) on data breach response strategies (DBRS). International Journal of Research and Innovation in Social Science, 9(14), 760-784.
27. Tamana, S., Yiangou, K., Orphanou, K., Chatzimatthaiou, S., Kountouris, P., & Cremonesi, F. (2026). FAIR data gaps and collaboration willingness among hemoglobinopathy research centers. Scientific Data, 13(1), 582.
28. Yang, J. (2026). Stage-Coupled Computational Framework for Stratified Accessibility and Equity Analysis in Community-Based Elderly Care Services.
29. Zhang, Z. (2026). A Study on Return Optimization in E-commerce for Complex Consumer Goods Driven by Installation Information Quality. Available at SSRN 6734720.
30. Myeong, S., & Kanzamanova, R. (2026). When digital trust collapses: an exploratory comparative framework for citizen involvement in digital governance. Humanities and Social Sciences Communications.