



Available Online at EScience Press
International Journal of Education Foundations
ISSN: 3078-7866 (Online), 3078-7858 (Print)
<https://ijef.esciencepress.net>

RESEARCH ARTICLE

Engagement in Data Protection Ethical Practices Among Users of Artificial Intelligence Systems in Higher Education Institutions in Mwanza City, Tanzania

^aCesylia Robert Shangal, ^aDemetria Mkulu, ^aRaymond Ndomba

^aDepartment of Education Foundations, St. Augustine University of Tanzania, P. O. Box 307, Mwanza, Tanzania

Corresponding Author

Cesylia Robert Shangal, Email: mnncesyl@gmail.com

Author's Contributions

All authors contributed equally to this research.

Article History

Received : November 18, 2025; Accepted: January 28, 2026; Published: March 14, 2026.

ABSTRACT

Data protection ethical practices represent the behavioral dimension of data privacy literacy the extent to which users actively take steps to safeguard their personal information when engaging with Artificial Intelligence (AI) systems. This study analysed users' engagement in data protection ethical practices when using AI systems in Higher Education Institutions (HEIs) in Mwanza City, Tanzania. An explanatory sequential design was employed, with 200 respondents consisting of 163 students and 37 academicians, surveyed through a five-point Likert scale questionnaire, supplemented by 6 key-informant interviews with institutional administrative staff. Descriptive statistics and Braun and Clarke's thematic analysis were applied to quantitative and qualitative data respectively. Findings revealed uniformly low engagement across all protective behaviours for both user groups. Among academicians, the most frequently practiced behaviour was checking privacy terms before recommending an AI tool (sometimes, often and always 48.6%), while informing students in the syllabus about AI data collection (sometimes, often and always: 18.9%) and consulting the Data Protection/Legal Office before deploying a new AI system (sometimes, often and always: 21.6%) were near-absent. Among students, the highest-engagement behaviour was avoiding uploads of personal files to public AI without checking policy (sometimes, often and always: 59.5%), while reporting suspicious data requests to the university was the least common (sometimes or more: 30.7%). The absence of institutional policies, Data Protection Officers, privacy training, and reporting mechanisms is identified as the structural cause of this poor engagement. The study recommends mandatory privacy training, institutional AI policy development, and a functioning Data Protection Officer (DPO) mechanism as urgent priorities for Mwanza HEIs.

Keywords: Data Protection, Engagement, AI Ethics, Higher Education

INTRODUCTION

Data privacy literacy is made up of three connected parts: understanding privacy laws and how Artificial Intelligence (AI) works, perception which means what people think about risks and benefits, and engagement which means the actual steps users take to protect their personal information. Most research on AI and privacy in higher education has focused on the first two areas.

However, engagement is what users actually do to safeguard their data, has not been studied enough, especially in Sub-Saharan Africa (Gomes, 2024; Al Shamsi et al., 2025). This is a serious gap because without knowing how users behave, Higher Education Institutions (HEIs) cannot design effective training or support, and policymakers cannot tell whether laws like

Tanzania's Personal Data Protection Act (PDPA, 2022) are making a real difference.

This study therefore asks a key question: To what extent do students and academicians in Mwanza's HEIs actually engage in ethical data protection practices when using AI? It looks at specific behaviours, such as reading privacy policies before using AI tools, adjusting privacy settings, removing personal details before uploading data to outside AI platforms, consulting Data Protection Officers, informing students about data collection, and reporting suspicious requests. These actions matter because 94.5% of users in the main study already use AI regularly (Shangali, 2026), yet Tanzania's PDPA requires both individuals and institutions to handle personal data carefully. The urgency of this issue is clear due to 2024, the HELLCAT ransomware group attacked a Tanzanian university and stole over 500,000 student records containing names and billing information (RedPacket Security, 2024). This real-world breach shows what can happen when data protection practices are weak. Pelletier et al. (2024) also warn that the rapid spread of AI tools increases users' exposure to data collection, making protective actions more important than ever.

Studies globally highlights the problem, in Peru, Marin et al. (2025) found that over half of students and academicians were worried about privacy and felt AI systems were not transparent. In Spain, Ciudad-Gomez (2024) reported that students had only limited understanding of AI ethics. In South Africa, Mutanga et al. (2024) found that privacy concerns were a major barrier to AI adoption. In Ghana, Owusu et al. (2025) showed that while educators were open to AI, poor infrastructure and training stood in the way. In Tanzania, Luhwera (2024) found positive attitudes toward AI's benefits, but did not examine data privacy literacy exactly the gap this paper fills. Mwamlangala (2025) and Luwavi and Kumbo (2025) both confirmed that Tanzanian HEIs lack policies, training, and Data Protection Officers, even though many individuals are using AI. To address these problems, this study offers actionable recommendations aligned with Tanzania's PDPA and National AI in Education Guidelines, aiming to support responsible AI adoption while protecting users' privacy rights. To note, engagement in data protection is not just about knowing the rules it is about taking real steps to protect personal information. Without understanding what users actually do, neither HEI nor policymakers can ensure that AI is used safely and responsibly.

LITERATURE REVIEW AND THEORETICAL FRAMEWORK

Theoretical Review

This study is grounded in complementary model and theoretical frameworks to explain the determinants of data protection engagement. The Technology Acceptance Model (TAM), formulated by Davis (1989),

posits that Perceived Usefulness and Perceived Ease of Use drive technology adoption. TAM predicts that when users find AI tools easy and useful, they will adopt them with minimal friction potentially bypassing privacy checks, consent reading, and protective settings adjustments in favor of task completion (Mambile & Mwongosi, 2024; Al Zaidy, 2024). This 'convenience over caution' dynamic is a recurring theme in educational AI literature.

Privacy Calculus Theory (Laufer & Wolfe, 1977; Meier & Krämer, 2024) provides a complementary lens: individuals disclose personal information when perceived benefits outweigh perceived privacy risks. Low engagement with data protection practices can therefore be understood as the behavioral consequence of underestimating privacy risks either because users do not know the risks exist, or because they perceive AI's utility as sufficiently high to justify sharing. Shouli et al. (2025), applying a Privacy Calculus model to AI privacy management, found that risk awareness is the primary moderator of protective behaviour: users who understand risks engage more consistently in protective practices. The absence of institutional training and disclosure obligations in Mwanza HEIs thus functions as a structural suppressor of the risk-awareness necessary to trigger engagement.

Empirical Review

Engagement in data protection practices represents the behavioral dimension of data privacy literacy, reflecting whether users translate their understanding and perceptions into protective actions when using AI systems. Studies across different contexts reveal a persistent gap between awareness of data protection principles and actual engagement in protective practices.

Globally, research on actual data-protection engagement as distinct from stated awareness or intention reveals consistently low rates. Gomes (2024), studying Spanish university students, found that limited ethics training correlated with low privacy-protective behaviour, even among students who expressed awareness of privacy risks. Al Shamsi et al. (2025), studying 50 students across 38 UAE institutions, found that while students could articulate recommended protective behaviours, they rarely enacted them in practice revealing a knowledge action gap. Al Zaidy (2024), examining generative AI use in US higher education, found students routinely using AI for grammar-checking 42% and information retrieval 69% without adjusting privacy settings, demonstrating TAM's predicted ease-of-use-first behaviour.

In Sub-Saharan Africa, Omariba (2025) found AI tools becoming routine in Kenyan HEIs 40% weekly, 30% daily, 20% monthly, and 10% rare usage but did not assess whether this frequent use was accompanied by protective behaviours a gap this study addresses. Mambile and Mwongosi (2024), examining AI adoption

in Tanzanian HEIs, found that while students are accepting of AI due to its effectiveness, neither students nor academicians demonstrated clear data protection habits. Maliganya and Mboshaa (2025), studying facilitators' strategies for managing AI in Tanzanian HEI assessment, found that lecturers lacked institutional guidance on how to communicate about AI data collection with students directly relevant to the engagement deficit documented in the present study. The structural drivers of low engagement are well-documented in the Tanzanian context. Mwamlangala (2025) found PDPA compliance across four Tanzanian HEIs to be extremely low, with no functioning Data Protection Officers (DPOs), no privacy training, and no formal reporting mechanisms. King et al. (2025), examining privacy policies of six major United State AI companies including Amazon, Anthropic, Google, Meta, Microsoft, and OpenAI found that all six use chat inputs to train their models by default, and some retain data indefinitely. This finding has direct implications for Tanzanian HEI users who upload identified student documents to these platforms without anonymization. This study directly examines this question by assessing actual engagement in data protection practices, providing evidence of whether responsible data protection behaviors accompany the positive attitudes and high usage reported in previous studies or whether there is a practice disconnect.

RESEARCH METHODOLOGY

This study adopted mixed research approach with an explanatory sequential mixed-methods design (Creswell & Creswell, 2023). It involved quantitative data collection from 200 respondents across two HEIs in Mwanza City: 163 students (response rate: 100%) and 37 academicians (response rate: 100%). Sample sizes were determined using Yamane's (1967) formula $n = N / (1 + N(e)^2)$, with a 7.5% margin of error for students and 8.5% for academicians, both at 95% confidence. Stratified sampling was applied to ensure proportional representation by gender, age, faculty, and year of study. The engagement objective was operationalised through two separate Likert-scale instruments: a four-item scale for academicians and a six-item scale for students, each rated on a five-point frequency scale (1 = Never to 5 = Always). Cronbach's alpha coefficients confirmed adequate internal reliability for the engagement subscales. I was also complemented by six semi-structured interviews with key informants involved 2 Deans, 2 Heads of Department (HOD), and two ICT Officers, purposively selected for their institutional authority over AI governance. Interviews were audio-recorded, transcribed verbatim, and analysed using Braun and Clarke's (2006) six-phase thematic analysis. Ethical clearance was obtained from SAUT's Institutional Review Board; participants were guaranteed anonymity and coded as Interviewee A,

Interviewee B and Interviewee C, and the right to withdraw without consequence.

RESULTS AND DISCUSSION

Academicians' Engagement in Data Protection Ethical Practices (n = 37)

Table 1 presents the frequency distribution of academicians' engagement across four protective behaviours. A clear hierarchical pattern was observed: behaviours requiring only individual action such as checking privacy terms are most common, while those requiring institutional coordination like consulting the data protection officer (DPO), informing students in the syllabus were almost not existed.

Table 1. Academicians' Engagement in Data Protection Ethical Practices (n = 37)

Statement	N%	R%	S %	O %	A%	Total %
Check privacy terms before recommending or testing an AI tool.	18.9	32.5	32.4	5.4	10.8	100
Department consults the data protection/legal office when deploying a new AI system.	64.9	13.5	16.2	5.4	0	100
Inform students in syllabus about data AI tools will collect.	73	8.1	13.5	5.4	0	100
Remove student names and IDs and pictures before using their data with external AI tool.	48.6	16.2	21.6	8.1	5.4	100

Source: Field Data (2026)

Checking privacy terms before recommending or testing an AI tool showed the highest engagement where by 32.4% reported doing so sometimes, 5.4% often, and 10.8% always a hence make a rate of

(48.6%). Yet the majority (51.4%) never or rarely conduct this check, meaning most AI tool recommendations reaching students originate from academicians who have not reviewed the associated privacy terms. This finding supported by Luwavi and Kumbo (2025) found a comparable pattern among academicians in Dar es Salaam: despite high AI awareness, formal governance was insufficient to guide responsible use. Similarly, Mambile and Mwongosi (2024) found that data privacy and security were major challenges of AI adoption, with academicians expressing concern about data handling. One of the interviewees claimed that:

I am aware of the restrictions on using AI tools. I accept the terms and conditions unless acceptance is not required. However, I am not sure about the students, since we have not communicated with them or recommended any specific tools. What we are trying to emphasize is that AI should only be used as an extra resource, in addition to the work they have been given. (Interviewee A, May 2026).

This implies that academicians risk student data and institutional legal compliance by recommending AI tools without reviewing privacy terms, breaching the Personal Data Protection Act of 2022. To address this, HEIs must implement privacy training, appoint a data protection officer to approve tools, and enforce consistent, vetted recommendations to reduce breach risks.

The data protection engagement collapse is most acute in institutional coordination behaviours. A number of 64.9% of academicians reported never consulting the Data Protection or Legal Office before deploying a new AI system, and not a single respondent (0%) reported always doing so. Mwamlangala (2025) confirms that the absence of DPOs a legal requirement under PDPA (2022) is characteristic of Tanzanian HEIs, making institutional consultation structurally impossible. Similarly, Mambile and Mwongosi (2024) found that data privacy and security were major challenges to AI adoption, and that a lack of institutional governance was a key factor. This represents not a failure of individual motivation but of institutional infrastructure. The qualitative data reveals why:

We have no communication about those experts; all in all, there is no clear solution for using AI. AI is there whether you like it or not; it is like the internet, it is inevitable. So, we need to find a proper way to use it without affecting the consumer's output. (Interviewee B, May 2026).

This finding implies that when a department deploys an AI system without consulting privacy experts, the HEI

may lose control over which student data is collected and how it is used. The researcher suggests that HEIs should review the PDPA document and establish a mandatory review process for any new AI system before it can be adopted.

The lowest-engagement behaviour among academicians was informing students in their course syllabi about the data an AI tool will collect: 73% reported never doing so, and 8.1% rarely a combined never/rarely rate of 81.1%. This near-total absence of syllabus disclosure violates the transparency principle articulated in Tanzania's National AI in Education Guidelines (MoEST, 2025), which explicitly require institutions to communicate to users what data AI systems collect and how. Maliganya and Mboshaa (2025) found that Tanzanian facilitators valued AI efficiency but lacked formal guidance on communicating with students about AI data collection the same institutional silence documented here. It also aligns with Barros et al. (2025), who found low awareness of data protection laws among HEIs in Brazil. The consequence is that students cannot give informed consent to AI data collection in their academic activities, directly violating the PDPA's consent provisions.

Regarding anonymisation, 48.6% of academicians reported never removing students' names and IDs before using their data with external AI tools, and 16.2% rarely a combined 64.8% who leave student data identifiable when uploading to external platforms. The findings show that the majority of academicians feed students' data into AI tools without removing names and IDs. This means if a data breach occurs at the AI company, students' information will be directly exposed. The risk is concrete to the HELLCAT breach in Tanzania (RedPacket Security, 2024) illustrates the real consequences of inadequate data anonymization in the HEI context after stolen of over 500,000 student records containing names and billing information.

Based on the findings and references, the researcher suggests that HEIs should provide training for academicians on removing identifying information before uploading students' documents. By doing this, academicians' and HEIs' reputations will be remain protected, even if any data leakage occurs, because they have been informed and see that HEIs have always taken precautions.

Students' Engagement in Data Protection Ethical Practices (n = 163)

Table 2 presents students' engagement across six protective behaviours. Students exhibit a comparable pattern to academicians' highest engagement in basic, individually-controlled behaviours and lowest engagement in those requiring institutional interaction.

Table 2. Students' Engagement in Data Protection Ethical Practices (n = 163)

Statement	N %	R %	S %	O %	A %	Total %
Read privacy terms before using a new AI tool for studies.	30.1	19	27.5	11.7	11.7	100
Change app privacy settings to limit data shared.	19.6	21.5	32.5	12.9	13.5	100
Avoid uploading personal files to public AI without checking the policy.	19	21.5	25.2	19	15.3	100
Ask the lecturer or IT staff what data AI collects before using it.	47.9	16	16.6	9.1	10.4	100
Remove name or other identifying details before using personal	29.4	20.9	25.8	12.3	11.6	100

data with public AI tools.

Report suspicion requests for personal data to the university	46	23.3	16.6	6.1	8	100
---	----	------	------	-----	---	-----

Source: Field Data (2026).

The most common protective action students took was avoiding uploading personal files to public AI tools without checking the policy first 59.5% said they did this sometimes or more often. The next most common was changing privacy settings, with 58.9% doing so sometimes or more often. These results suggest that students have a basic instinct to protect themselves, which fits with Privacy Calculus Theory of 1977: students act when the privacy risk is obvious, like when they are about to upload personal files. One student wrote in the open-ended survey: "Sometimes I think I do not trust AI system, I think they might be using some of our data and privacy. I am always concerned about data privacy and how my personal information is shared when using AI tools" (Survey Student, April 2026). However, there is also evidence of what Technological Acceptance Model (Davis, 1989) calls ease-of-use override, meaning that when AI is very convenient, students skip protective steps. For example, 40.5% said they never or rarely avoid uploading without checking the policy.

Reading privacy terms before using a new AI tool showed even lower engagement: 49.1% said they never or rarely do this, and only 23.4% said they do it often or always. This matches what Ciudad-Gomez (2024) found among Spanish university student, very few actually read privacy policies. This might be because the policy is long and complex to read, or because they are simply accepting it to solve their problems (Barros et al., 2025; Ciudad-Gomez, 2024). TAM explains this well: students care most about ease and usefulness, and long privacy documents feel like a hassle, so most people do not bother reading them. HEIs have a duty under Tanzania's PDPA (2022) and the National AI Guidelines (MoEST, 2025) to turn these long documents into short, easy-to-understand summaries and to include privacy education in student orientation programmes.

The two least common protective behaviours both involved interacting with the institution. Asking lecturers

or IT staff about data collection was something 63.9% said they never or rarely did. They may not know that this is something they should ask about, or they might feel shy or embarrassed to ask. This is also supported by the Mwamlangala (2025) study, which examined compliance with the PDPA of 2022 in HEIs and found it to be extremely low. And reporting suspicious data requests to the university was even lower 69.3% said they never or rarely did this, with 46% saying they never did it at all. An interviewee acknowledged that:

There is no any incident of student come to us for asking what AI data are collected or reporting a problem with AI. Maybe because it is not authorised, but in reality, when you report that you have used AI on assignment or research, it is totally identified you as a bogus. (Interviewee C, May 2026).

This response shows a double problem: students are afraid they will be punished if they tell their lecturers they use AI, and there is no safe, non-punitive way for them to report data privacy worries. The PDPA of 2022 (URT, 2023) requires universities to have systems for handling complaints about data privacy violations, but this requirement has clearly not been put into practice. The behaviour of removing identifying details before using personal data with public AI tools showed that 50.3% said they never or rarely do this. This means half of students are regularly uploading personal information that can be identified back to them onto public AI platforms that, as King et al. (2025) show, keep and use this data by default. Privacy Calculus Theory suggests this happens because students underestimate the risk: they focus on the immediate benefit, like finishing assignments faster, and don't really think about the possibility of a data breach, their content being used to train the AI, or the data being shared with third parties (Laufer & Wolfe, 1977)

Generally, study found that the lack of data protection among users in Mwanza's HEIs is not because people are lazy or do not care. Instead, it is caused by institutional failures. HEIs are missing several key things: clear AI and privacy policies, Data Protection Officers (which the PDPA requires), formal privacy training for staff and students, safe ways for students to report concerns without fear of punishment, and rules that require lecturers to tell students how their data will be used.

If these things were in place, they would directly improve engagement. Policies would tell people what is expected. Data Protection Officers would give users someone to ask for advice. Training would help users understand risks which Privacy Calculus Theory says is what motivates people to protect themselves. And reporting channels would give students a safe way to exercise their rights. Without these supports, both students and academicians end up using AI frequently

but with very little protective behaviour. This pattern is predictable, it breaks the law, and it can be fixed if Mwanza HEIs take targeted action.

CONCLUSION AND RECOMENDATION

This study looked at how students and academicians in Mwanza's HEIs engage in ethical data protection practices when using AI. Both groups showed low and uneven engagement across all protective behaviours measured. The actions they took most often were basic, personal precautions like checking policies before uploading files and changing privacy settings. The actions they took least often were those that required help from the institution, such as getting syllabus disclosures, consulting a Data Protection Officer, or reporting incidents. The main reason for this low engagement is not individual laziness but structural failures: HEIs lack policies, Data Protection Officers, training programmes, and reporting mechanisms. All of these are required by Tanzania's PDPA of 2022 and the Tanzanian National AI Guideline in Education, but none of the HEI studied have put them in place.

The study suggests the following priority actions. HEIs should immediately appoint and make known a Data Protection Officer, and create a safe, protective channel for reporting AI data concerns. All academicians should be required to complete annual training on PDPA rules, how to anonymise data, and the privacy policies of AI tools approved for HEI use. Academicians should also include a statement in every course syllabus that explains what data AI tools collect and how students can protect themselves. When HEIs buy new AI tools, procurement teams and Data Protection Officers should check them against a privacy checklist first. Students should be educated through orientation and clear policies on how to read privacy terms, adjust settings, anonymise data before uploading, and report concerns without fear of punishment. Finally, the Ministry of Education (MoEST) and the Tanzania Commission for Universities (TCU) should require regular PDPA compliance audits and enforce the 2024 AI in Education Guidelines.

REFERENCES

- Al Shamsi, S., Al Mamami, R., Ali, S. & El Sayary, A. (2025). Impact of AI Usage Ethically on Students. Proceeding of the 16th International Conference on Society and Information Technologies (ICSIT 2025). pp. 55-62 <https://doi.org/10.54808/ICSIT2025.01.55>
- AL Zaidy, A. (2024). The Impact of Generative AI on Student Engagement and Ethics in Higher Education. Journal of Information Technology, Cybersecurity and Artificial Intelligence, 1 (1), 30-38. <https://www.researchgate.net/publication/385498725>
- Barros, Y. C., Vilela, J. (2025). Data Privacy in

- Educational Contexts: Analysing Perceptions, Practices and Challenges in Personal Data Protection. 27th International Conference on Enterprise Information Systems, (2)308-319. DOI:10.5220/0013426900003929
- Braun, V., Clarke, V., & Hayfield, N. (2024). Thematic analysis: A reflexive approach. In J. A. Smith (Ed.), *Qualitative Psychology: A Practical Guide to Research Methods* (4th ed.). SAGE Publications.
- Ciudad-Gomez, A. (2025). Perception and Ethical Use of Artificial Intelligence by University Students. *Journal of Management and Business Education*, 8(1)18-36. <https://doi.org/10.35564/jmbe.2025.0002>
- Creswell, J. W., & Creswell, J. D. (2023). *Research Design: Qualitative, Quantitative and Mixed Method Approaches*. 6th Edition. SAGE Publication, Inc.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340. <https://doi.org/10.2307/249008>
- King, J., Chin, C., & Kulkarn, S. (2025). User Privacy and Large Language Models. Stanford Institute for Human Centered AI. <https://hai.stanford.edu/research/user-privacy-large-language-models>
- Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, 33(3), 22–42. <https://doi.org/10.1111/j.1540-4560.1977.tb01880.x>
- Luhwera, M.G. (2024). The Use of Artificial Intelligence in Tanzania's Higher Education: Instructors' Perceptions and Experiences at TPSC. *Journal of Public Sector Management* 8, 73-86. <https://jpsm.tpsc.go.tz/index.php/jpsm/article/view/30>
- Luwavi, E.O., & Kumbo, L.I. (2025). Bridging the Gap Between AI Tool Adoption and Institutional Readiness in Academic Writing and Review Practices Among Higher Learning Institution in Dar es Salaam, Tanzania. *East African Journal of Education and Social Sciences*, 6(6), 16-25. <https://doi.org/10.46606/99s2fz65>
- Maliganya ,W., & Mboshaa,M.A.(2025). Assessment of Facilitators' Strategies for Managing Artificial Intelligence. Challenge in Higher Education Assessment and Evaluation in Tanzania. *Business Excellence and Management*. 15(5), 225-243
- Mambile, C., & Mwogosi, A. (2024). Transforming Higher Education in Tanzania: Unleashing the True Potential of AI as a Transformative Learning Tool. *Technological Sustainability*, 4, 51-76. DOI:10.1108/TECHS-03-2024-0014
- Meier, Y. & Kramer, N. (2024). The privacy Calculus Revisited: Empirical Investigation of Online Privacy Decision Between and Within Person's Levels. *Communication Research*. 51(2),178-202. DOI:10.1177/00936502221102101
- Ministry of Education, Science and Technology (MoEST). (2025). *National Guidelines for Artificial Intelligence in Education*. Dodoma: United Republic of Tanzania.
- Mutanga, B. M., Jugoo, V. & Adefeni, K. O. (2024). Lecture Perceptions on the Integration of Artificial Intelligence Tool into Teaching Practice. *Journal of Trends in Higher Education*. 3,1121-1133 <https://doi.org/10.3390/higheredu3040066>
- Mwamlangala, D.F. (2025). Are Universities Compliant? A Study of Tanzania's Personal Data Protection Act in Higher Learning Institution. *African Journal of Law and Practice*. 1(2), 66-83
- Omariba, A. (2025). Enhancing Student Outcome Through I Driven Personalized Learning: A study on Implementation and Effectiveness at the University in Kenya. *East African Journal of Education Studies Vol* 8,512- 529 <https://doi.org/10.37284/2707-3947>
- Owusu, P. K., Louis, D.K., Akwetey, J. D., Owusu, G. A., Koffie-Ocloo, D., Nuerthey, M. L., Arkhurst, A. V., & Asampanbilla, J. K. (2025). An Analysis of University Teachers' Perspectives on Using Generative Artificial Intelligence Tools in Higher Education: Evidence from. 17th International Conference of Education and New Technologies Palma, Spain. pp.1117-1123. <https://doi.org/10.21125/edulearn.2025.0358>
- Pelletier, K., Robert, J., Muscanell, N., MC Cormack, M., Reeves, J., & Arbino, N. (2024). *EDUCASE Horizon Report: Teaching and Learning Edition*. EDUCASE. <https://www.learntechlib.org/p/222401/>
- RedPacket Security. (2024). *HELLCAT Ransomware Victim: College of Business-Tanzania*.<https://www.breachsense.com/breaches/college-of-business-tanzania-data-breach/>
- Shangali, C. R. (2026). Assessing data privacy literacy in the application of Artificial Intelligence in Higher Education Institutions in Mwanza City, Tanzania [Master's dissertation]. St. Augustine University of Tanzania.
- Shouli, A., Berthwal, A., Compbell, M., & Shrestha. (2025). Unpacking Youth Privacy Management in AI Systems: A privacy Calculus Model Analysis. *IEEE Access Publication*.
- United Republic of Tanzania (URT). (2022). *The Personal Data Protection Act, 2023*. Government Printer. The Special Gazette of the United Republic of Tanzania No. 15 Vol. 104. The Government Printer.