Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Assessing the Legal Challenges of Artificial Intelligence Use in Children's Education in Tanzania

Winfrida Emanuel Mroso[1]

Resident Magistrate
Judiciary of Tanzania

DOI: https://doi.org/10.63363/aijfr.2026.v07i06.8624

Abstract
This article examines the legal challenges related to the use of artificial intelligence in children's education in Tanzania. It asks whether the existing legal framework protects children from risks arising from AI use in the learning process. The article invokes doctrinal methodology, while analysing the legal framework, international and regional instruments and scholarly literature relevant to the study. It finds that, although Tanzania has enacted laws on child protection, education and personal data protection and a National Guidelines for Artificial Intelligence in Education (2025), the law remains far from addressing AI-specific risks affecting children in education, which include personal data protection, consent, automated decision-making, algorithmic bias, transparency and accountability. The article recommends the adoption of clear, child-centred regulatory standards for AI use in education, supported by oversight and accountability mechanisms. It concludes that Tanzania's emerging AI governance framework must expressly address children's rights and educational contexts.

Keywords: Artificial Intelligence; Children's Education; Legal Challenges; Child Rights; Data Protection; Tanzania

1. Introduction

Artificial intelligence (AI) is changing how teaching, learning and educational administration are understood and organised. Its educational applications include intelligent tutoring systems, adaptive learning platforms and tools that analyse learners' progress. These technologies offer opportunities to support individualised learning and assist teachers, while increasing the role of learner data in educational processes.[2] Their evaluation nevertheless requires attention to the purposes of education, the importance of human judgement and the relationships through which children learn.[3]

The legal significance of these developments becomes particularly pronounced where learners are children. Children's engagement with digital technologies involves interconnected interests in protection,

[1] LLB Hons, Mzumbe University, LLM students at the Open University of Tanzania.
[2] W Holmes, M Bialik and C Fadel, *Artificial Intelligence in Education: Promises and Implications for Teaching and Learning* (Center for Curriculum Redesign 2019).
[3]

participation and access to educational opportunities. Consequently, an assessment of educational AI must consider both its potential benefits and its implications for children as independent rights holders.[4] The United Nations Committee on the Rights of the Child expressly recognises that children's rights must be respected, protected and fulfilled in the digital environment, which includes artificial intelligence, automated systems, data analytics and biometrics.[5]

One central concern is the collection and processing of information about learners. AI-enabled educational systems may analyse learning activities, performance and interactions with digital platforms to construct learner profiles or recommend educational interventions. Although such analysis can support teaching, it raises questions about privacy, autonomy and the purposes for which educational information is subsequently used.[6]Where AI influences assessment or other decisions affecting learners, additional concerns arise about fairness, transparency, accountability and the possibility of unintended harm.[7]

In Tanzania, these concerns engage existing constitutional protections. Article 13 of the Constitution of the United Republic of Tanzania establishes equality before the law and protections against discrimination, while Article 16 protects privacy and personal security.[8] These provisions provide a constitutional foundation for examining whether educational technologies subject children to unjustified intrusion or unequal treatment. The relevant legal inquiry therefore extends beyond the accuracy or efficiency of an AI system to the compatibility of its operation with protected rights.

The Law of the Child Act provides more specific protection for children's welfare and educational interests. Applicable in Mainland Tanzania, the Act defines a child as a person under eighteen years and makes the child's best interests a primary consideration in specified actions concerning children. It also prohibits discrimination, protects access to education and recognises a child's right to express an opinion and participate in decisions affecting the child's well-being. [9]These standards provide a basis for assessing whether AI-assisted monitoring, assessment or educational intervention respects children's welfare and participation.

Educational governance is also relevant. The Education Act regulates matters including school management, compulsory enrolment and attendance, curricula and school inspection.[10] AI use in schools consequently raises questions about how existing educational responsibilities should operate when institutions rely on technological systems supplied or managed by external providers. Inclusion requires particular attention because the Persons with Disabilities Act contains protections concerning education and accessibility for persons with disabilities.[11] An assessment of educational AI should therefore examine whether its design and use support equitable participation, including participation by children with disabilities.

The Personal Data Protection Act, 2022 supplies a further legal framework for examining the processing of children's information. Particularly significant is section 36, which addresses decisions that

4

5 UN Committee on the Rights of the Child, 'General Comment No 25 (2021) on Children's Rights in Relation to the Digital Environment' (2 March 2021) UN Doc CRC/C/GC/25, paras 2–4.

6 Holmes, Bialik and Fadel (n 1); W Holmes and others, 'Ethics of AI in Education: Towards a Community-Wide Framework' L

7 Ibid

8

9 Law of the Child Act 2009, Cap 13 RE 2023 ('Law of the Child Act'), ss 2, 4, 5, 8 and 11.

10 Education Act 1978, Cap 353 RE 2023, ss 34–35 and 38–42.

11 Persons with Disabilities Act 2010, Act No 9 of 2010.

significantly affect a data subject and are based solely on automated processing. It provides mechanisms for requiring that such decisions not rest solely on automatic processing and for requesting reconsideration, subject to specified exceptions.[12] The Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023 elaborate operational safeguards, including procedures for exercising data-subject rights, provisions addressing the exercise of rights on behalf of children and requirements concerning data-protection impact assessments.[13] These provisions make it necessary to investigate how legal safeguards apply in educational relationships involving children, parents, schools and technology providers.

Safeguarding objectives do not remove the need for scrutiny. A technological intervention intended to protect a learner may nevertheless involve disproportionate monitoring, inaccurate classification or discriminatory consequences. Educational AI scholarship emphasises that beneficial intentions alone do not ensure responsible design or deployment.[14] Correspondingly, the Committee on the Rights of the Child calls for standards ensuring that digital educational technologies do not expose children to discrimination, misuse of personal data, commercial exploitation or other infringements of their rights.[15]

Against this background, this article assesses the legal challenges arising from actual or prospective AI use in children's education in Tanzania. It examines whether applicable protections adequately address privacy, children's participation, automated decision-making, educational inclusion, accountability and remedies. The article's central argument is that educational AI requires an integrated legal assessment connecting data protection with children's welfare and educational rights. Its analysis distinguishes the relevant territorial jurisdictions: the Law of the Child Act applies to Mainland Tanzania, while the Personal Data Protection Act excludes non-union matters in Zanzibar from its application.[16] The article seeks to identify the protection available under existing law and the areas in which clearer rules or implementation measures may be required.

2. State of the Literature

Five works from the selected literature are especially relevant to this inquiry: Ally's analysis of Tanzanian educational governance, Bennett Moses's account of legal adaptation, Krafft and others' examination of regulatory definitions, Mittelstadt's critique of principle-based AI governance, and Adams's study of children's understandings of childhood. Together, they provide a basis for examining how legal problems should be identified, how regulatory responses should be organised and whose perspectives should inform those responses.

Ally's 'Artificial Intelligence and Education Governance in Tanzania: Legal Gaps and Regulatory Challenges' provides the closest connection to the present study. Using doctrinal and comparative analysis, Ally evaluates Tanzanian legal and policy instruments against international and regional approaches to educational AI. The article identifies shortcomings in regulatory coherence, institutional oversight and accountability, and recommends a comprehensive binding framework for AI in education.[17] Its principal contribution is to place educational AI within Tanzania's regulatory institutions rather than treating governance as an abstract international concern. However, the present article must move beyond a general

[12] Personal Data Protection Act 2022, Act No 11 of 2022, Cap 44 ('Personal Data Protection Act'), s 36(1)–(3).
[13] Ibid
[14] Holmes and others (n 5).
[15] UN Committee on the Rights of the Child (n 4) para 103.
[16] Law of the Child Act, s 2; Personal Data Protection Act, s 2.
[17] Ally AM, 'Artificial Intelligence and Education Governance in Tanzania: Legal Gaps and Regulatory Challenges' (2025) 17

diagnosis of regulatory gaps. It asks which existing duties protect children, how those duties interact and whether particular problems arise from deficient legislation, uncertain interpretation or weak implementation. This narrower inquiry can test the extent to which comprehensive new legislation is necessary, rather than assuming that legislative novelty is itself the appropriate response.

Bennett Moses's 'Agents of Change: How the Law "Copes" with Technological Change' supplies a useful framework for making that distinction. The article examines how Australian institutions respond to technological change, identifying contributions from courts, parliamentary committees, government departments, law-reform organisations and other bodies. [18]Its significance lies in challenging an undifferentiated account of law as simply falling behind technology. Legal adaptation involves several institutions and methods, each with different capacities and limitations. Applied to educational AI in Tanzania, this approach directs attention to the institutions capable of clarifying duties, investigating complaints and developing regulatory standards. Nevertheless, the latter institutional experience cannot establish the competence or effectiveness of Tanzanian bodies. The article offers an analytical method that requires local examination, particularly of overlapping mandates and coordination. It also provides a counterpoint to Ally: before proposing a new framework, the assessment should identify what existing institutions can achieve and where their authority is insufficient.

Krafft and others address a prior difficulty in 'Defining AI in Policy versus Practice': identifying the technologies to which governance measures should apply. Through surveys of researchers and analysis of policy documents, they find a difference between definitions emphasising technical functionality and those comparing systems with human thought or behaviour. They argue that the latter approach may direct attention towards hypothetical future technologies while overlooking systems already in use.[19]This contribution matters because an assessment of legal adequacy depends on a clear account of the activity being regulated. For this article, their findings support examining systems through their functions and effects, including prediction, classification and decision support. However, definitional clarity does not determine the appropriate legal safeguard. Systems performing similar functions may create different risks depending on their educational purpose and consequences. The study therefore assists with identifying the scope of inquiry but must be supplemented by a contextual assessment of children's educational relationships.

Mittelstadt's 'Principles Alone Cannot Guarantee Ethical AI' shifts the discussion from regulatory scope to regulatory effectiveness. He questions whether agreement on broad ethical principles can produce responsible practice without supporting institutions, methods and accountability mechanisms. His comparison with medical ethics identifies difficulties arising from the absence of shared professional foundations and established means of translating principles into operational requirements.[20]The article's contribution is particularly valuable when evaluating recommendations framed around fairness, transparency or responsibility: such terms need identifiable duties, responsible actors and procedures for assessing compliance. For the present study, this suggests examining whether educational governance measures specify who must act, what action is required and what follows from non-compliance. Its limitation is its general treatment of AI development. The article does not itself resolve how accountability

[18] L Bennett Moses, 'Agents of Change: How the Law "Copes" with Technological Change' (2011) 20(4) *Griffith Law Review.*
[19] PM Krafft and others, 'Defining AI in Policy versus Practice' in *Proceedings of the 2020 AAAI/ACM Conference on AI, Ethics, and Society* (Association for Computing Machinery 2020
[20] B Mittelstadt, 'Principles Alone Cannot Guarantee Ethical AI' (2019) 1 *Nature Machine Intelligence* .

should be distributed between educational authorities, schools and technology providers. That allocation requires analysis of the relevant legal relationships.

Adams's 'What Is a Child? Children's Perceptions, the Cambridge Primary Review and Implications for Education' adds a perspective that institutional and regulatory scholarship can overlook. Drawing on a study involving 56 children aged seven to eleven, Adams examines how children understand childhood. Their responses reflect agency and relational understandings, alongside biological development and movement towards adulthood.[21] The study's contribution is to question whether adult-defined categories adequately represent children's experiences. Applied to educational AI, it suggests that consultation should account for differences in children's understanding rather than presume either complete incapacity or uniform competence. However, the study concerns primary education in England and does not investigate AI or Tanzanian children. Its findings therefore support a methodological commitment to hearing children's perspectives, rather than a direct conclusion about local attitudes or legal capacity.

These works reveal a productive tension between calls for comprehensive regulation and the need to diagnose particular legal and institutional deficiencies. Ally identifies problems within Tanzanian educational governance; Bennett Moses encourages scrutiny of available mechanisms of adaptation; Krafft and others clarify the importance of regulatory scope; Mittelstadt tests the practical force of governance principles; and Adams questions whose understanding informs educational decisions.[22] The present article brings these perspectives together through a child-specific legal inquiry. Its contribution is to distinguish gaps in legal coverage from difficulties of interpretation, institutional coordination and enforcement, while considering whether affected children can participate meaningfully in the processes designed to protect them.

The reviewed literature provides a useful starting point for understanding the legal challenges of AI use in children's education. It shows that the adequacy of a legal framework cannot be judged simply by the presence or absence of legislation. Attention must also be paid to how existing rules apply to particular technologies, whether institutions understand and fulfil their responsibilities, and whether those affected can obtain a remedy when something goes wrong. The literature also highlights the importance of understanding children's experiences rather than relying entirely on adult assumptions about their needs and abilities.

These insights guide the present article's assessment of Tanzania's legal framework. The discussion examines whether existing laws provide clear and workable protection for children, how responsibilities are shared among educational authorities, schools and technology providers, and where difficulties arise in interpretation or enforcement. It also considers whether children and their parents have meaningful opportunities to question AI-assisted decisions and seek redress. This approach allows the article to identify where existing protections can be strengthened and where additional legal measures may be necessary.

[21] K Adams, 'What Is a Child? Children's Perceptions, the Cambridge Primary Review and Implications for Education' (2014) 44(2) *Cambridge Journal of Education*

[22]

3. Methodology

This study adopts a doctrinal legal research methodology to assess the legal challenges of artificial intelligence use in children's education in Tanzania. It examines the content, scope and interaction of applicable legal rules to determine how they protect children and allocate responsibility for AI-related harm. This approach is appropriate because the study seeks to establish what the law provides, identify uncertainties in its application and assess whether further legal clarification or reform is necessary.

The analysis draws on primary and secondary legal sources. Primary sources include the Constitution of the United Republic of Tanzania, legislation and subsidiary legislation concerning education, children's welfare, personal data protection, disability rights and digital activities. Relevant judicial decisions are considered where they assist in interpreting these provisions. International and regional instruments concerning children's rights provide additional interpretive benchmarks, with attention to their legal status and domestic applicability. Secondary sources comprise scholarly books, journal articles and relevant research publications that explain the relationship between law, technology and educational governance.

Sources are selected according to their relevance to the study's central questions. The analysis focuses on provisions governing children's rights, the collection and processing of personal information, automated decision-making, educational inclusion, institutional duties and remedies. Each provision is examined in its statutory context and read alongside related laws. The study distinguishes binding legal obligations from policy guidance and scholarly recommendations, and takes account of differences in territorial application between Mainland Tanzania and Zanzibar.

The assessment proceeds by relating these legal provisions to particular functions that AI may perform in education, such as analysing learner information, supporting assessment and informing educational interventions. It considers whether existing rules cover these activities, whether the duties of schools and technology providers are sufficiently clear, and whether affected children can challenge decisions or obtain redress. This enables the study to distinguish gaps in legal coverage from uncertainties of interpretation and questions that depend on implementation.

The study does not collect empirical data through interviews, questionnaires or observation. It therefore does not establish how widely AI is used in Tanzanian schools or measure compliance with existing law. Examples of educational AI are used to examine possible legal consequences, rather than as evidence of local deployment. Its conclusions concern the adequacy and application of the legal framework; findings about institutional practice or children's experiences would require separate empirical research.

4. Legal Framework Governing AI Use in Children's Education in Tanzania

Several Tanzanian laws provide a basis for assessing AI use in children's education. Some protect children's rights directly, while others govern schools, personal information, digital communications and access to remedies. Each law contributes to the framework, although its scope and purpose determine how far its protection extends. The discussion below examines these provisions and their respective limitations.

4.1 Constitution of the United Republic of Tanzania, 1977

The Constitution of the United Republic of Tanzania protects human dignity, equality before the law, privacy and personal security. It also recognises fair-hearing requirements and access to an appeal or another legal remedy when rights and duties are determined by a court or another agency.[23] These

[23] Constitution of the United Republic of Tanzania 1977 (as amended), arts 12, 13(1)–(6) and 16.

protections provide a foundation for examining educational decisions involving AI, particularly where they affect a child's treatment or involve the use of personal information.

The Constitution also addresses access to education and the Government's responsibility to promote equal educational opportunities. However, these commitments appear among the fundamental objectives and directive principles of state policy, which are not directly enforceable by courts.[24] This distinction matters: the constitutional commitment to education should not be presented as having the same direct enforceability as the basic rights concerning equality and privacy.

The Constitution's limitation in this context is its broad character. It establishes fundamental standards but does not explain how schools should evaluate an AI system, communicate its operation to children or review its recommendations. Giving practical effect to these constitutional protections therefore requires supporting legislation and interpretation.

4.2 Law of the Child Act, 2009

The Law of the Child Act provides direct protection for children in Mainland Tanzania. It recognises the best interests of the child, prohibits discrimination and protects access to education. It also recognises the right of a child capable of forming views to express an opinion, be listened to and participate in decisions affecting the child's well-being.[25]

These protections are relevant when schools introduce technologies that monitor children, assess their performance or influence educational support. A school's decision to use AI must be considered alongside its responsibilities towards the children affected. The right to participation also means that communication with parents should not automatically replace opportunities to hear the child's own views.

The Act nevertheless leaves important procedural details open. Its general protections do not explain how a child should receive information about an AI system, question an automated classification or participate in a review of its use. The limitation is therefore not an absence of children's rights, but a lack of detailed guidance on applying those rights within technology-assisted educational processes.

4.3 Education Act, 1978

The Education Act provides the framework for school management and educational supervision. It addresses compulsory enrolment and attendance, school boards and committees, approved curricula and syllabi, and school inspection.[26] These provisions offer an existing structure through which educational practices involving AI can be examined.

The Act is important because the introduction of technology does not remove a school's responsibility for the education it provides. Learning materials and instructional practices involving AI must still be considered within the school's educational and administrative obligations.

Its limitation is that the general framework does not itself provide a detailed procedure for evaluating educational AI. The provisions examined do not specify how automated assessment systems should be tested, how their performance should be reviewed or how teachers should document reliance on their recommendations. Existing management and inspection powers provide a foundation, but their application to particular AI functions requires clarification.

[24] Ibid, arts 7(2) and 11.
[25] Law of the Child Act, ss 2, 4, 5, 8 and 11
[26] Education Act 1978, Cap 353 RE 2023, ss 34–35 and 38–42

4.4 Tanzania Institute of Education Act, 1975

The Tanzania Institute of Education Act assigns the Institute responsibilities for developing and evaluating educational programmes, reviewing curricula and syllabi, and specifying standards for equipment, instruments and other devices used for educational purposes.[27]

These responsibilities are relevant to the educational suitability of AI tools. They provide a basis for considering whether a proposed technology supports curricular objectives and is appropriate for teaching and learning. However, the extent to which particular software falls within the statutory reference to educational devices requires interpretation.

The Act does not expressly establish a specific approval process for educational AI. It does not state what evidence should demonstrate a system's suitability, how often it should be reassessed or how changes to its operation should be reviewed. The Institute's mandate is therefore important, but it should not be treated as proof that every AI tool already undergoes a defined statutory approval process.

4.5 Persons with Disabilities Act, 2010

The Persons with Disabilities Act protects equal educational participation in Mainland Tanzania. It recognises rights to education and training in inclusive settings, equal school-admission rights for children with disabilities and appropriate support services. It also places learning institutions under an obligation not to discriminate against persons with disabilities.[28]

These protections matter where AI is used to deliver learning materials or assess children's performance. Technology should be examined in light of the institution's existing responsibility to provide inclusive education. Its introduction cannot justify excluding a learner or withholding necessary support.

The Act provides a substantive standard, but does not itself prescribe technical requirements for educational AI. It does not expressly explain how systems should be tested across different disabilities or how interfaces and assessment methods should accommodate particular needs. This leaves institutions with general duties that must be translated into practical requirements for each system. The lack of technical detail does not make inaccessible or discriminatory technology legally acceptable.

4.6 Personal Data Protection Act, 2022

The Personal Data Protection Act is central to educational AI that relies on information about children. It treats data relating to children as sensitive personal data and establishes requirements concerning lawful and transparent processing, specified purposes, necessary collection, accuracy and security. It also addresses consent through legally recognised representatives where the data subject is a minor, alongside specified exceptions.[29]

The Act further provides rights concerning information about the logic involved in certain automated decisions. Where a significantly affecting decision is based solely on automated processing, it provides notification and reconsideration safeguards, subject to exceptions.[30]

These protections are substantial, but their scope requires care. The safeguard concerning decisions based solely on automated processing does not expressly cover every decision informed by AI. The legal effect of human involvement therefore requires interpretation. The exceptions also mean that the protection is not absolute. More broadly, compliance with data-protection law does not establish that an AI system is

[27] Tanzania Institute of Education Act 1975, Cap 142 RE 2023, ss 3–4
[28] Persons with Disabilities Act 2010, Act No 9 of 2010, ss 2 and 27–28
[29] Personal Data Protection Act, ss 3, 5 and 30

educationally suitable. The Act protects information and related rights, while educational quality requires additional assessment.

4.7 Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023

The Personal Data Protection (Personal Data Collection and Processing) Regulations give practical effect to the Act. They address the exercise of rights on behalf of children, information provided to parents or guardians, notification of automated decisions and human intervention to reduce bias. They also require prior data-protection impact assessments for specified processing, including children's sensitive data, biometric information and certain automated decisions.[30] The subsequent amendments require sensitive personal data to be kept separately from other personal data.[31]

These measures provide safeguards before processing begins, as well as procedures for exercising rights afterwards. Their limitation is their primary focus on data protection. An assessment of processing risks does not, by itself, establish whether a tool supports learning or meets curricular requirements.

The representative safeguards also do not provide a detailed process for involving children personally. The Regulations therefore need to be read alongside with the Law of the Child Act and applicable educational responsibilities, so that protecting a child's information does not overshadow the child's participation and educational interests.

4.8 Cybercrimes Act, 2015

The Cybercrimes Act protects against unlawful conduct involving computer systems. It addresses offences including unlawful access, interception, interference with data and systems, computer-related forgery and fraud, identity-related crimes and cyberbullying. It also prohibits specified conduct involving material categorised by the Act as child pornography, including images representing children engaged in sexually explicit conduct.[32]

These provisions may become relevant where educational systems are attacked, learner records are unlawfully altered or prohibited material is distributed through digital platforms. Their application depends on proving the elements of the particular offence. Harmful material or an inaccurate output does not automatically become a criminal offence because AI was involved.

The Act's limitation is its criminal-law purpose. It does not establish a general system for evaluating the quality of educational AI. An unfair assessment or unsuitable recommendation may require correction even where no criminal offence can be established. Criminal protection therefore supports the wider framework but cannot replace educational supervision or data-protection safeguards.

4.9 Electronic and Postal Communications Act, 2010

The Electronic and Postal Communications Act regulates communications services and content. It provides for content standards aimed at protecting children and the public from harmful material. It also addresses educational content and accessibility for persons with sight or hearing impairments.[33]

[30] Personal Data Protection (Personal Data Collection and Processing) (Amendment) Regulations 2024, GN No 808 of 2024, reg 5.
[31] Ibid
[32] Cybercrimes Act 2015, Cap 443 RE 2023, ss 3–9, 11–13, 15, 23 and pt IV
[33] Electronic and Postal Communications Act 2010, Cap 306 RE 2023, ss 103–104 and 110–111.

These provisions are relevant where an educational service falls within the activities regulated by the Act. They provide a basis for considering the quality, suitability and accessibility of content delivered through regulated services.

Their limitation lies partly in their scope. A school-based tool does not necessarily become a regulated content service simply because it uses AI or connects to the internet. Its activities and legal classification must first be examined. The content provisions also do not establish a general procedure for reviewing automated assessments or learner classifications. The Act consequently governs an important part of the digital environment without addressing every educational use of AI in the same way.

4.10 Commission for Human Rights and Good Governance Act, 2001

The Commission for Human Rights and Good Governance Act provides an avenue for addressing alleged rights violations and maladministration. It authorises the Commission to receive complaints, conduct inquiries, advise institutions and, where necessary, institute court proceedings. It also provides for complaints and representation.[34] These functions may assist children affected by unfair treatment involving educational AI.

However, the Commission's decisions have the status of recommendations. The relevant authority must report on the action taken, and an inadequate response may lead the Commission to bring court proceedings or recommend that a competent authority do so.[35]

This makes the Commission an important oversight body, although its recommendations should not be equated with directly executable court orders. Its general human-rights mandate also does not itself create a technical certification process for educational algorithms. Its contribution is principally to investigate complaints, promote compliance and support remedial action.

Together, these laws provide a substantial foundation for protecting children when AI is used in education. Their limitations differ according to their purposes: some establish broad rights, while others govern educational institutions, personal information, prohibited conduct or remedies. This framework provides the basis for the later assessment of legal challenges, particularly how these protections operate together and where further clarification may be needed.

4.11 National Guidelines for Artificial Intelligence in Education, 2025

The National Guidelines for Artificial Intelligence in Education, issued by the Ministry of Education, Science and Technology in January 2025, address responsible AI development and use across education, including pre-primary, primary and secondary schooling. They require stakeholders to align institutional policies with the Guidelines. Their inclusion is therefore essential to understanding Tanzania's approach to AI in children's education.[36]

The Guidelines address privacy, informed consent, bias auditing and institutional responsibility for monitoring AI use. These expectations give schools a basis for assessing whether educational technologies treat learners fairly and protect their information. They also call for accessible tools and learning environments that accommodate children with disabilities.[38]

[34] Commission for Human Rights and Good Governance Act 2001, Cap 391 RE 2023, ss 6 and 23–24.
[35] Ibid.
[36] Ministry of Education, Science and Technology, *National Guidelines for Artificial Intelligence in Education* (January 2025) paras 1.2 and 1.4, 3–5

Their principal limitation concerns enforcement. Although expressed in mandatory language, the Guidelines do not themselves establish a statutory compensation scheme or a dedicated appeal procedure for children affected by AI decisions. This study therefore treats them as administrative guidance whose practical protection depends on implementation and the applicable law. Their broad consent provisions also leave schools needing more specific procedures for involving children and parents in decisions about data collection.[37]

5. Legal Challenges

In Tanzania, the use of AI in education is regulated indirectly through general laws relating to children, education, personal data, disability and cybercrime. The principal laws include the Constitution of the United Republic of Tanzania[38], the Law of the Child Act[39], the Education Act[40], the Personal Data Protection Act, the Persons with Disabilities Act and the Cybercrimes Act[41] These laws provide important protection for children. However, they were not enacted specifically to govern artificial intelligence in educational institutions. This creates uncertainty regarding the legal responsibilities of schools, teachers, education authorities and technology providers. This chapter examines the principal legal challenges arising from the application of AI for safeguarding children in education in Tanzania.

5.1 Absence of a Specific and Binding Legal Framework Governing Artificial Intelligence in Education

The first legal challenge is the absence of a specific and binding legal framework governing the development, procurement and use of artificial intelligence in Tanzanian educational institutions. Tanzania has laws that regulate education, child welfare and personal data, but no single statute comprehensively addresses the use of AI in schools.

The Guidelines seek to promote the effective, ethical, secure and responsible use of artificial intelligence in the education sector.[42] They provide administrative direction to educational institutions and other stakeholders regarding the adoption of AI technologies. However, guidelines do not ordinarily have the same legal force as an Act of Parliament or regulations made under statutory authority. They may provide standards of good practice, but their violation may not automatically result in the same legal sanctions that would arise from violating binding statutory provisions. This may make it difficult to enforce the Guidelines against a school or technology provider that introduces an unsafe or inappropriate AI system.

The absence of binding AI-specific legislation means that legal protection must be obtained from different statutes. For example, section 4(2) of the Law of the Child Act requires the best interests of the child to be a primary consideration in every action concerning a child undertaken by public or private institutions and administrative bodies.[43] This provision applies to decisions by schools and education authorities to introduce AI systems that process children's information or affect their education and welfare.

[37] Ibid.
[38] Cap 2 R.E 2002
[39] Cap 13 R.E 2023
[40] *Education Act*, Cap 353, R.E. 2023
[41] Cap 443, R.E. 2023
[42] Ministry of Education, Science and Technology, *National Guidelines for Artificial Intelligence in Education*.
[43] *Law of the Child Act*, Cap 13, R.E. 2023, s 4(2).

The Law of the Child Act also protects children from discrimination and conduct that may injure their physical or mental well-being.[44]However, the Act does not expressly regulate algorithmic discrimination, automated learner profiling, biometric surveillance, educational chatbots or AI-supported disciplinary decisions.

The Education Act provides the general legal framework for the administration, supervision and management of educational institutions in Tanzania. It gives the Minister responsible for education powers concerning the implementation of education policy and the regulation of educational institutions.[45] Nevertheless, the Act does not contain detailed provisions governing the use of artificial intelligence in schools.

5.1.2 Limited Protection of Children's Personal Data and the Limitations of Consent

Another legal challenge arising from the application of artificial intelligence for safeguarding children in education is the protection of children's personal data. Artificial intelligence systems normally depend on the collection, storage and analysis of large amounts of information. In educational institutions, such information may include a learner's name, age, photograph, fingerprint, voice recording, examination results, attendance records, disability information, health information, online activities and behavioural patterns.

Some AI systems used for safeguarding may process particularly sensitive information. For example, a system designed to identify children who may require psychological support may analyse a learner's behaviour, communications, attendance and academic performance. A biometric attendance system may process fingerprints or facial images, while online examination-proctoring software may record a learner's face, voice, home environment, computer activity and movements during an examination.

The Personal Data Protection Act,[46] Section 3 of the Act defines personal data broadly and specifically classifies information relating to children and biometric information as sensitive personal data. This classification provides an important level of protection because children may not fully understand the consequences of the collection and continued use of their information. Section 5 of the Act requires personal data to be processed lawfully, fairly and transparently.[47] It must be collected for an explicit, specified and legitimate purpose and must be limited to information that is necessary for that purpose. The information must also be accurate, securely protected and retained only for the period required to achieve the stated purpose. [48] These principles apply directly to educational institutions using artificial intelligence. A school should not collect every category of learner information merely because an AI system has the technical capacity to process it. The institution must first determine which information is genuinely necessary for the educational or safeguarding purpose.

Although parental consent is an important safeguard, it may not provide proper protection in an educational environment. Consent is legally meaningful only where the person giving it has adequate

[44] Ibid.
[45] *Education Act*, Cap 353, R.E. 2023, ss 4 and 5.
[46] *Personal Data Protection Act*, 2022, Cap 44, s 3
[47] Ibid.
[48] Ibid s. 5.

information and a genuine opportunity to accept or refuse the proposed processing. In practice, parents may be presented with a standard consent form stating that a school intends to use a digital learning platform, biometric attendance system or online examination application. The form may not clearly explain how the AI system operates, the information it collects, the period for which the information will be retained or whether the information will be transferred outside Tanzania. Consequently, obtaining parental consent should not mean that the child is completely excluded from the decision. Children should be informed, in language appropriate to their age and level of understanding, when an AI system will collect or analyse their information.

5.1.3 Automated Decision-Making and Inadequate Human Oversight

Another legal challenge is the use of artificial intelligence to make or influence decisions affecting children in educational institutions. AI systems may be used to detect examination misconduct, assess academic performance, identify behavioural problems or determine whether a learner requires special support. However, such systems may produce inaccurate or discriminatory results.

Section 36 of the Personal Data Protection Act,[49] protects a data subject against decisions that significantly affect them where those decisions are based solely on automated processing. It also allows the affected person to request reconsideration of the decision.[50] Section 33 further provides a right to information about the logic involved in an automated decision.[51]

The main limitation is that these provisions apply mainly to decisions made solely by automated means. A school may claim that a teacher made the final decision even where the teacher merely accepted the AI recommendation without independent assessment. Meaningful human oversight requires the responsible teacher or education officer to examine the evidence, understand the limitations of the AI system and have the authority to reject its recommendation. A learner should not be suspended, expelled, accused of examination cheating or denied educational support solely because of an AI-generated result.

Regulation 31(e)[52] of the regulation requires human intervention to minimise bias arising from automated decision-making.[53] The Law of the Child Act also requires the best interests of the child to be a primary consideration and gives children capable of forming views a right to participate in decisions affecting them.[54] Therefore, Tanzania should adopt education-specific rules requiring human review before any significant AI-supported decision is implemented. The affected learner and parent or guardian should also receive an understandable explanation and an opportunity to challenge the decision.

5.1.4 Cybersecurity and Data-Breach Risks

Another legal challenge is the risk of unauthorised access, loss or disclosure of children's information. AI systems used in schools may store photographs, biometric information, examination records, health information and behavioural data. A security breach involving such information may expose children to identity theft, discrimination, embarrassment or other forms of harm.

[49] Personal Data Protection Act, 2022, Cap 44, s 36.
[50] Ibid
[51] Ibid.
[52] *Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023*
[53] Ibid
[54] *Law of the Child Act*, Cap 13, R.E. 2023, ss 4(2) and 11.

Section 27 of the Personal Data Protection Act, 2022[55] requires data controllers and processors to establish reasonable technical and organisational safeguards against loss, destruction, alteration and unauthorised access to personal data. The 2023 Regulations also require access controls, secure storage, audit trails, breach-management procedures and regular testing of software vulnerabilities. However, some educational institutions may lack trained personnel, secure computer systems and sufficient resources to comply with these obligations. Schools may also depend on external technology providers without adequately examining their security arrangements.

The Cybercrimes Act criminalises unlawful access, interception and interference with computer systems and data.[56] Nevertheless, criminal law mainly applies after an offence has occurred. It does not remove the responsibility of schools to prevent security breaches before deploying AI systems.

Educational institutions should therefore conduct security assessments, limit access to learner information and ensure that contracts with technology providers contain clear obligations concerning cybersecurity, breach notification and deletion of information. Schools should not introduce AI systems that collect sensitive information unless they have the capacity to protect it.

5.2 Legal Lacuna in Data Protection

The findings revealed that there is a legal lacuna in the regulation of AI educational technologies that collect sensitive information such as student performance, behaviour, voice, facial images, and online learning patterns. Through a doctrinal analysis of the Personal Data Protection Act, the provision of section 5 of the Act[57] has established principles of lawful and fair processing of personal data, but it does not provide special provisions specifically designed for children's data in AI environments. The Act also lacks detailed rules concerning parental consent, profiling of minors, and automated educational monitoring. The Act has only provided for the control the flow of data by requiring all those wanting to collect or produce data to register.[58] Consequently, schools and digital learning companies may process children's data without sufficient safeguards. This creates risks of privacy violations, unauthorised data sharing, and exploitation of children's digital identities. The absence of child-specific AI data protection standards, therefore, remains a serious legal weakness within the Tanzanian framework.

5.2.1 Legal Institutional Limitation

The findings revealed the presence of Legal Institutional Limitation in regulating AI in the education system. The researcher identified the existence of multiple institutions in place but none is legally tied to the regulation of AI, children and education at once. The TCRA has been limited by law to protect the interests of consumers in the digital market.[59] It is not clear whether the consumer interests fall under AI or not. The researcher identified that the Personal Data Protection Commission is limited in monitoring compliance against data Controllers and data processors in Tanzania and not tied to AI platforms in the education sector.[60] On the part of the Tanzania Institute of Education, the Institute has limited powers to only undertake analysis, review and revision of curricula and syllabi in Tanzania and does not have powers

[55] Cap 44 R.E 2023
[56] *Cybercrimes Act*, Cap 443, R.E. 2023.
[57] Findings obtained by documentary review conducted on the Tanzanian Personal Data Protection Act, Cap 44 RE 2023
[58] Ibid S. 6
[59]Ibid S. 5 (1) Para (b)
[60]Findings obtained by documentary review conducted on the Tanzanian Personal Data Protection Act, Cap 44 RE 2023, S. 7 Para (a)

to control the usage of AI by children in schools.[61] Lastly, the Tanzania National Commission for Science and Technology is confined into serving as the principal advisory organ to the government of Tanzania in regards to research and technological developments, but does not have regulatory powers on AI usage in schools by children.[62] The researcher confirmed that there is a need to have a single institution that regulates and governs AI in Tanzania.

5.2.2 Non-Enforcement of AI Violations

The findings revealed that there is a challenge in the enforcement mechanisms' capacity to supervise AI technologies used in schools. Thus, the researcher identified that there is no clear legal provision of law that provides for who enforces AI infringements against children who are using it for educational purposes. The enforcement challenge comes due to two aspects. Due to the jurisdictional issues of AI platforms that are operating in Tanzania, they don't have offices in Tanzania and they are foreign based that making it difficult to enforce the law against them.[63]Secondly, although the police force is in place for the maintenance of law and order in the territory of the United Republic of Tanzania,[64] there is no clear mandate in law that empowers the police force to enforce AI infringements against children using it in the education sector in Tanzania. Thus, the researcher confirmed that the enforcement of AI in Tanzania is paramount.

5.2.3 Judicial Jurisprudential Limitations

The findings revealed that Tanzania experiences a challenge arising from the lack of judicial precedents and comprehensive AI jurisprudence. Tanzanian courts have not yet developed substantial case law addressing liability, negligence, discrimination, or privacy violations caused by AI educational technologies. In technological advancement in Tanzania, it was the Judiciary that came with a case law that eventually led to the amendments of the law. This can be obtained from a prominent case of Trust Bank Tanzania v Lemash Enterprises Limited;[65] in this case, the Court was of the view that electronic evidence is admissible before the Courts of Law in Tanzania. This led to the amendment of the best evidence rule due to technological advancements.[66] But this has not been the case in the AI industry, where the Court is silent and has not provided a judicial guideline on the protection of children using AI for educational purposes. The researcher confirms that the lack of established AI-related case law, therefore, limits the development of strong legal standards capable of protecting children in modern digital learning environments in Tanzania.

[61] Findings obtained by documentary review conducted on the Tanzania Institute of Education Act Cap 142, RE 2023, S. 4 Para b

[62] Findings obtained by documentary review conducted on the, Tanzania National Commission for Science and Technology Act Cap 226, RE 2023 S. 5 (1)

[63] The Findings obtained by way of documentary review on the establishment of Open AI, Gemini, ChatGpt and Caprot in Tanzania.

[64]The Findings obtained by way of documentary review on the Police Force and Auxiliary Services Act Cap 322, RE 2023, S. 5 (1) Para c

[65] The Findings obtained by way of documentary review on the High Court Judgments, in the High Court of Tanzania Commercial Case No 4 of 2000

[66] The Findings obtained by way of documentary review on the Tanzania Evidence Act Cap 6 RE 2023, S. 70 (1)

5.2.4 Non-Comprehensive AI Policy

The findings also revealed that there is an absence of a comprehensive AI policy in Tanzania. This becomes a challenge in the safeguarding of children using AI in their education process. This is because the existing ICT policies were developed before the rapid growth of generative AI technologies. The National ICT Policy of 2016 encourages the use of digital technology in education and national development, but it does not address ethical AI governance, transparency, or child online safety in AI-based learning systems.[67]

5.2.5 Non-Comprehensive AI Policy

The findings also revealed that there is an absence of a comprehensive AI policy in Tanzania. This becomes a challenge in safeguarding children using AI in their education process. This is because the existing ICT policies were developed before the rapid growth of generative AI technologies. The National ICT Policy of 2016 encourages the use of digital technology in education and national development, but it does not address ethical AI governance, transparency, or child online safety in AI based learning systems.[68]

6. Recommendations

The protection of children in AI-supported education requires clearer legal standards, practical safeguards within schools and effective avenues for obtaining redress. Reform should build on Tanzania's existing protections for children, personal data and education, while addressing the particular risks created by AI. The aim should be to enable educational innovation under conditions that preserve children's dignity, safety and equal opportunity to learn.

6.1 Establishing Binding Standards for AI Use in Education

Tanzania should develop binding standards governing the selection, procurement and use of AI in educational institutions. The National Guidelines for Artificial Intelligence in Education provide a starting point, but their expectations should be translated into enforceable duties through legislation or regulations made under appropriate statutory authority. These duties should apply to public and private educational institutions and clearly distinguish the responsibilities of schools, education authorities and technology providers.

The standards should reflect the level of risk posed by each use. An application that helps a teacher prepare learning materials should receive different scrutiny from a system that monitors children's behaviour or influences disciplinary decisions. Before introducing systems with significant implications for children, institutions should assess their educational necessity, reliability and effects on children's rights. Where a less intrusive method can achieve the same purpose, the institution should explain why AI is nevertheless required.

6.2 Strengthening Protection of Children's Personal Data

Education-specific data protection standards should explain how schools may collect, use, retain and share children's information through AI systems. They should address parental authorisation, children's participation, biometric information, learner profiling and the use of educational data for purposes beyond

[67] Findings obtained by documentary review conducted on the Tanzania National ICT Policy of 2016.Para 5.8, 35
[68] Ibid.

schooling. Schools should collect only the information needed for a clearly identified purpose and establish definite retention periods.

Consent procedures should also become more meaningful. Parents should receive understandable information about what a system collects, who can access the information and how it will be used. Children should receive explanations suited to their age and understanding. Where participation is optional, refusal should not unfairly restrict access to education, and a reasonable alternative should be available. Technology providers should not be permitted to reuse children's information for advertising or unrelated model training merely because a school has purchased their services.

6.3 Ensuring Human Review and Fair Treatment

Schools should retain responsibility for decisions affecting a child's academic progress, discipline and access to support. AI outputs should inform professional judgment rather than determine outcomes automatically. Before acting on a consequential recommendation, the responsible teacher or officer should examine the underlying evidence, consider the child's circumstances and have the authority to reject the recommendation.

Children and their parents should receive understandable reasons for adverse decisions and a practical opportunity to challenge them. Review procedures should allow errors to be corrected promptly, particularly where a decision could interrupt schooling or damage a learner's reputation. Teachers should therefore receive training that enables them to recognise unreliable outputs and assess the limits of the systems they use.

Fairness should also be examined before deployment and throughout a system's use. Testing should consider Tanzanian languages, disability, age and differences in learners' social and educational circumstances. Procurement agreements should require providers to supply sufficient information for schools and regulators to evaluate accuracy and discriminatory effects. Systems that repeatedly disadvantage particular groups should be corrected, suspended or withdrawn.

6.4 Improving Security and Technology Procurement

Schools need practical support to protect the information entrusted to them. Education authorities should develop procurement standards and model contractual terms covering security, access controls, breach reporting, data retention and deletion. Contracts should also clarify responsibility where a provider relies on subcontractors or stores information outside Tanzania.

These requirements should be accompanied by resources and technical assistance, particularly for schools with limited infrastructure. Introducing a sophisticated system without the capacity to secure it can undermine the protection it promises. Institutions should therefore assess their readiness before deployment and periodically review whether their security arrangements remain adequate.

6.5 Clarifying Institutional Responsibility and Access to Remedies

Tanzania should establish a clear arrangement for coordinating oversight of educational AI. Education authorities, the Personal Data Protection Commission and other relevant bodies should have defined responsibilities for receiving complaints, sharing information and responding to incidents. A designated coordinating body could help prevent complaints from being passed between institutions without resolution. Creating an entirely new regulator should depend on whether existing institutions, with clearer mandates and adequate resources, can perform this role effectively.

Complaint procedures should be accessible to children and parents, inexpensive and capable of producing timely outcomes. Available responses should include correcting inaccurate records, reviewing affected decisions and stopping harmful processing. Contracts with foreign providers should establish clear contact points and cooperation duties, while preserving remedies available under applicable law.

Judicial and regulatory capacity should also be strengthened. Training on automated decision-making, digital evidence and children's rights would help decision-makers address disputes involving unfamiliar technologies. Relevant decisions should be published with appropriate protection of children's identities so that schools and providers can understand and apply the developing standards.

6.6 Sustaining Policy Development and Children's Participation

AI policy should be reviewed regularly as educational practices and technologies change. Reviews should involve teachers, parents, children, disability organisations and specialists in education, law and technology. Children's participation is particularly important because they experience the effects of these systems directly, yet may have little influence over their introduction.

Implementation should be monitored through evidence of how systems affect learning, privacy and equal treatment. This would help policy move beyond statements of principle towards standards that schools can apply and authorities can enforce.

7. Conclusion

This study has examined whether Tanzania's legal and policy framework adequately protects children when AI is used in education. Its central conclusion is that existing protections provide a foundation, but their application to educational AI requires greater clarity and stronger implementation. General duties concerning child welfare, equality and data protection must be translated into practical expectations for the institutions that select, operate and supply these technologies.

The National Guidelines for Artificial Intelligence in Education are an important part of that process. Their value will depend on whether schools can put their expectations into practice and whether children can obtain effective remedies when those expectations are not met. Legal reform should therefore proceed alongside institutional coordination, teacher training and support for schools with limited technical capacity.

AI should ultimately be assessed by how it serves the child. Greater efficiency or more detailed information about learners does not alone justify intrusive monitoring or decisions that are difficult to challenge. A sound framework should allow useful technologies to improve education while ensuring that children remain heard, fairly treated and protected. Tanzania's task is to make those protections a consistent part of everyday educational practice.