CIPESA Submission to the Draft Kenya Artificial Intelligence and other Emerging Technologies Policy, 2026

Submitted to the Committee on Artificial Intelligence and other Emerging Technologies, State Department for ICT and the Digital Economy, Republic of Kenya, August 2026

August 4, 2026

The Chairperson
Committee on Artificial Intelligence and other Emerging Technologies
C/O Principal Secretary, State Department for ICT and the Digital Economy
10th Floor, Telposta Towers
P.O. Box 30025-00100, Nairobi, Kenya
By email: aipolicy@moict.go.ke; cc: legal@moict.go.ke

Dear Sir,

RE: SUBMISSION ON THE DRAFT KENYA ARTIFICIAL INTELLIGENCE AND OTHER EMERGING TECHNOLOGIES POLICY, 2026

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA) welcomes the opportunity to comment on the Draft Kenya Artificial Intelligence and other Emerging Technologies Policy, 2026 ("the Policy"), published for public participation by the State Department for ICT and the Digital Economy. CIPESA works across East and Southern Africa to advance digital rights, evidence-based AI governance, and open, accountable internet policy. CIPESA is pleased to comment on the Draft Kenya Artificial Intelligence and other Emerging Technologies Policy, 2026.

Kenya's Policy is among the most detailed AI governance frameworks yet produced on the continent, and several of its provisions could potentially set a standard other African states are likely to reference as they develop their own frameworks. The draft Policy is critical for fostering a holistic national framework that guides the development, deployment, governance, and use of AI and other Emerging Technologies in Kenya. Furthermore, the policy contains several strong provisions, particularly regarding environmental disclosure and protections for AI value chain workers.

This submission proposes amendments to the Policy to better align with the African Union (AU) Continental Artificial Intelligence Strategy (2024), the UNESCO Recommendation on the Ethics of Artificial Intelligence, and Kenya’s constitutional commitments to accountable governance and the protection of fundamental rights. The areas of focus for redress include: oversight institutions; state use of AI for security purposes; reliance on the future Governance Act; transparency and accountability; scope gaps, including democratic integrity; and gender-based harms. The primary aim of this submission is to prescribe additional safeguards or implementation measures to ensure responsible AI adoption and usage in the country.

The enclosed memorandum sets out our proposed recommendations for your consideration across the Policy's institutional, rights, fiscal, and implementation provisions, together with the rationale.

We would welcome the opportunity to discuss any part of this submission with the Committee.

Yours sincerely,

CIPESA Team

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA)				
S/No	**Section of the Policy**	**Provisions of the Policy**	**Proposed Amendment**	**Rationale for Amendment Recommendation**
1.	Section 3.1.1 and Section 3.1.2	The policy commits to the development of a national R&D Data Repository and promotion of indigenous AI models	Amend Section 3.1.1 to ensure inclusion of regional dataset pooling and cross-border research collaborations, e.g., with AU Member States and regional research networks, including joint training-data consortia for African languages. Add a sub-section on establishing and training datasets within the AU. This would foster regional LLMs and language processing	The AU Continental AI Strategy and AU Data Policy Framework call for pooled, interoperable African data infrastructure to reduce dependence on foreign-owned training data and compute. Kenya's domestic data pool is too small on its own to train competitive indigenous language models at scale; regional pooling with linguistically related markets, e.g., within the East African Community (EAC), for example, would materially improve the viability of this objective.
2.	Section 4.2 and 4.2.1, Coordination Framework and Institutional Structure	Implementation is overseen through a four-tier structure headed by the Steering Committee, chaired by the Cabinet Secretary for MICDE. The Committee sets strategic direction and approves key frameworks and work programmes. The Council, a tier below, "shall submit annual reports to MICDE and Parliament while exercising independent regulatory judgment within its statutory mandate," but operates inside a structure headed by the same ministry it is meant to hold to	Guarantee the Council's independence, including through direct reporting to Parliament or another independent oversight arrangement, and give it powers to audit, obtain information and issue compliance directions. The proposed AI and other Emerging Technologies Governance Act[1] should also establish independent audits for high-risk AI systems, clear responsibilities across the AI	The AU Strategy emphasises institutional mechanisms capable of oversight, accountability, compliance monitoring and redress. A Council led by the same ministry it is meant to hold accountable may struggle to exercise independent oversight. Kenya's challenge is not developing rules but ensuring an independent institution can oversee their implementation. As currently drafted, the structure risks duplication of effort, ambiguity at county level, and weakened policy coherence**.** Independent

[1] Under Section 3.5.1, the Policy commits the government to develop a dedicated AI and other Emerging Technologies Governance Act to provide the legal framework for AI and other Emerging Technologies governance in Kenya, including the establishment, powers, and functions of the Council.

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA)				
S/No	**Section of the Policy**	**Provisions of the Policy**	**Proposed Amendment**	**Rationale for Amendment Recommendation**
		account.	lifecycle, and effective remedies for non-compliance. Clarify and specify the leading regulating entity as opposed to the several structures that potentially create ambiguities in implementation. The Committee should also explore how to leverage existing regulators, as opposed to creating new centres that do not effectively address the fragmentation that is rampant in the regulation and governance of the ICT sector.	audits, lifecycle responsibilities and enforcement powers give the Council something concrete to act on. The policy proposals on regulation as they are could potentially lead to duplication of efforts and roles,result in poor implementation, and undermine policy coordination and coherence.
3.	Section 4.2.2, Multi-Agency Roles; Section 3.7.6, Security, Defence and Public Safety	The National Police Service, the Directorate of Criminal Investigations and the Kenya Defence Forces are included under the Policy's list of "Regulatory Agencies" in section 4.2.2. Section 3.7.6 provides safeguards for lethal autonomous weapons, including the principle that fully autonomous systems without human control over lethal force are not acceptable. But for domestic surveillance, biometric identification and predictive policing, the Policy commits only to	Require independent approval and a published human rights impact assessment before deploying biometric identification or predictive-policing systems. For real-time biometric surveillance and mass facial recognition in public spaces, apply a presumption against deployment unless there is a clear, narrowly defined law-enforcement need.	The AU Strategy names unlawful surveillance among AI's core risks in Africa, and the African Commission on Human and Peoples' Rights has recognised AI's human rights impacts. Kenya's National Police Service already operates facial recognition on live CCTV feeds in Nairobi and Mombasa, with plans to expand to other cities. The response to the 2024 Finance Bill protests illustrates the importance of robust safeguards governing digital surveillance and law enforcement technologies, particularly

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA)				
S/No	**Section of the Policy**	**Provisions of the Policy**	**Proposed Amendment**	**Rationale for Amendment Recommendation**
		"establish safeguards" with no authorisation requirement or oversight body.		where AI-enabled systems may be deployed. This would provide stronger safeguards for the highest-risk uses without imposing a blanket prohibition on legitimate policing.
4.	Section 3.5.6(4), Public-Sector AI Adoption and Procurement Framework; Section 4.3.2, County AI and Data Readiness Framework	The Policy commits to "maintain a public register of AI and other Emerging Technologies systems deployed by public institutions, subject to appropriate exceptions for national security and law enforcement where disclosure would create a demonstrable risk". This is also provided for in county deployments, in Section 4.3.2.	Require independent review of any decision to withhold an AI system from the public register, with statutory time limits on non-disclosure and periodic reporting to Parliament on the number and categories withheld.	The AU Strategy supports public disclosure as the default, with exceptions requiring justification and oversight. CIPESA's regional research shows that broad national security exemptions can reduce transparency around state surveillance systems and make independent scrutiny more difficult.[2] An unreviewed exception risks becoming the rule rather than the exception in practice.
5.	Section 1.4.2, Policy Objective 7; Section 1.6.6, Guiding Principle 6; Section 4.5.4(10)	The Policy commits to developing "accessible grievance, appeal, and dispute resolution mechanisms" as one of 19 elements the future Governance Act must contain, without naming the body, process or timeline for lodging a complaint.	Design and establish a dedicated AI complaints and redress mechanism in the proposed AI Governance Act, with a public complaints portal and clear statutory timelines for investigations and responses.	The AU Strategy is explicit that independent institutions must provide access to redress and effective remedy. Likewise, the UNESCO Recommendation recognises access to remedy and accountability as essential components of trustworthy AI governance. A right to redress without a clear named forum, procedure and timeline is difficult to exercise, particularly where the detail is deferred to regulations that do not yet exist.

[2] CIPESA, State of Internet Freedom in Africa 2025: Kenya Country Report http://cipesa.org/download/reports/State_of_Internet_Freedom_in_Africa_2025___Navigating_the_Implications_of_AI_on_Digital_Democracy_in_Kenya__.pdf ; CIPESA, State of Internet Freedom in Africa 2025: Regional Report http://cipesa.org/download/reports/State_of_Internet_Freedom_in_Africa_Report_.pdf

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA)				
S/No	**Section of the Policy**	**Provisions of the Policy**	**Proposed Amendment**	**Rationale for Amendment Recommendation**
6.	Section 3.3.5, Protection of AI Value-Chain Workers; Section 4.5.4(12)	The Policy already contains strong protections for AI value chain workers, including safeguards against harmful content exposure, access to mental health support, transparent contracting practices, proportionate workplace surveillance measures, and accessible grievance and redress mechanisms listed among the required elements of the future Governance Act.	CIPESA welcomes this provision and recommends that the AI Governance Act makes clear that foreign companies commissioning data annotation and content moderation work are accountable where they influence working conditions, not only domestic sub-contractors that formally employ the workers.	The AU Strategy identifies labour protections for gig and platform workers as a regulatory gap. The joint statement by the Global Digital Justice Forum and Global South Alliance, which CIPESA has helped bring to African policy audiences, notes that conditions are set by the commissioning client, not the local intermediary, as Kenyan data annotators and content moderators illustrate directly. Accountability provisions that stop at the domestic sub-contractor would miss the party actually setting the terms of work.
7.	Section 1.1.1, Overview of AI and other Emerging Technologies; Section 4.5.2, Key International Conventions, Treaties and Frameworks; Section 5.12, Policy Review and Adaptation	The AU Continental AI Strategy is named in the Policy's introduction alongside Agenda 2063[3] and the AU Data Policy Framework, and again at Section 4.5.2, helping "guide continental cooperation and implementation of African priorities." Section 5.12 provides a formal review every three to five years, but none of the criteria is tied to AU Strategy alignment.	Require that each formal policy review under section 5.12 include an explicit assessment of the extent to which this Policy and its implementation remain aligned with the AU Continental AI Strategy. The National AI and other Emerging Technologies Council shall publish the findings of that assessment together with the review report.	The AU Strategy is now in its implementation phase; the AU Commission and Smart Africa have described the current stage as moving "from adopting a common framework to delivering tangible outcomes," and the AU Commission has committed to track how member states are domesticating it over time.

[3] Agenda 2063 is the African Union's blueprint and master plan for transforming Africa into "the global powerhouse of the future".

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA)				
S/No	**Section of the Policy**	**Provisions of the Policy**	**Proposed Amendment**	**Rationale for Amendment Recommendation**
8.	Section 1.5.1, Technology Scope; Section 1.5.2, Actor and Jurisdictional Scope	The scope provisions list vendors, cloud providers, compute providers, model providers and data intermediaries. Nowhere, including Annex IV's definitions, are recommender systems, content curation algorithms or platform ranking systems named as standalone categories requiring registration, risk classification or transparency obligations. Section 1.5.2 extends jurisdiction territory to non-resident entities	Include recommender and content curation systems within the Policy's scope and require major digital platforms operating in Kenya to disclose information about their ranking and content moderation systems through the National AI Registry. Amend Section 1.5.2 to align cross-border data transfer provisions explicitly with the AfCFTA Digital Trade Protocol and the AU Data Policy Framework (2022).	For many Kenyans users, ranking and recommendation systems are their main interaction with AI, not only chatbots. CIPESA's 2025 State of Internet Freedom in Africa research found these systems shape how Kenyans access news and engage in public debate, and that AI-based content moderation is largely built for the Global North, forcing over 90% of Africans to switch to a dominant or colonial-era language to use major platforms of systems shaping information access. There is a risk of overlaps between the AfCFTA Digital Trade Protocol and the AU Data Policy Framework 2022, which restrict cross-border transfer and ensure alignment with the extra-territorial regulation
9.	Section 1.5.1, Technology Scope; Section 1.5.2, Actor and Jurisdictional Scope	The scope provisions are silent on AI-generated political content and synthetic media, falling outside the illustrative categories the Policy names.	Bring AI-generated political content and synthetic media within the Policy's scope, requiring transparency obligations, including labelling or equivalent disclosure mechanisms for synthetic political content where technically feasible.	The AU Strategy identifies disinformation as a distinct AI risk on the continent. Recent public events in Kenya illustrate the influence of online information ecosystems on democratic participation, and growing use of generative AI in political communication increases the importance of transparency around synthetic media. Kenya's 2022 elections already saw deepfake

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA)				
S/No	**Section of the Policy**	**Provisions of the Policy**	**Proposed Amendment**	**Rationale for Amendment Recommendation**
				audio of a presidential candidate and TikTok-amplified disinformation targeting ethnic communities, and dedicated analysis of AI regulation ahead of the August 2027 election has already flagged the absence of transparency rules for AI-generated campaign content.
10.	Section 4.2.1, National AI and other Emerging Technologies Steering Committee (Composition); Section 4.2.1, Technical Working Groups (Composition)	The Steering Committee, the apex body approving cross-cutting frameworks and annual work programmes, comprises the Cabinet Secretary for MICDE as Chair, other Cabinet Secretaries, and county, private-sector and research representation. Civil society is not listed. Technical Working Groups, one tier below, include civil society.	Add a civil society seat to the Steering Committee, and provide defined civil society representation on the Council's Governing Board or Technical Advisory Forum. This is to ensure multistakeholder representation exists where frameworks and programmes are actually approved.	The AU Strategy calls for meaningful participation of all stakeholders in AI governance, not only in implementation forums. The UNESCO Recommendation similarly emphasises inclusive, multi-stakeholder governance that enables meaningful participation by civil society, academia and affected communities.
11.	Section 3.4.1, Environmental Accountability Framework; Section 3.8.7, Renewable Energy Disclosure	The Policy already requires "disclosure of material environmental indicators for high-impact AI and other Emerging Technologies infrastructure and compute activity, including electricity consumption, water use, cooling methods, emissions basis, and end-of-life equipment management," with graduated thresholds and standardised reporting, and	CIPESA welcomes this provision and recommends independent third-party verification of environmental disclosures, with verified information published through the public Registry.	The AU Strategy names water scarcity from data centre cooling, carbon emissions and e-waste as material AI risks in Africa. Self-reported disclosures may limit reliability and comparability; verification and public access would turn a strong provision into one supporting genuine public accountability.

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA)				
S/No	**Section of the Policy**	**Provisions of the Policy**	**Proposed Amendment**	**Rationale for Amendment Recommendation**
		separately requires disclosure of energy sources.		
12.	Section 4.5.3, Key Legislative Proposals; Section 1.5.8, Participatory Implementation Principle	Many of the substantive protections this submission and the AU Strategy call for are deferred to the future Governance Act, which Section 4.5.3 commits to drafting within six months and enacting within 12 months. The draft Policy is ambitious in principle but dependent on that legislation for effective implementation.	State expressly that the draft AI Governance Act will undergo its own dedicated public participation process of no less than 30 days before submission to Parliament, separate from consultation on this Policy.	Because many of the Policy's key safeguards depend on the future Act, its drafting process will be critical to Kenya's alignment with the AU Strategy and UNESCO Recommendation. The AU Strategy's call for open consultation is not fulfilled by consultation on the Policy alone if the Act is drafted without the same standard.
13.	Section 5.4, Baseline Values, Indicators and Targets; Annex II, Monitoring and Evaluation Matrix	The indicators in Annex II are almost entirely institutional and output measures: directorates staffed, guidelines gazetted, systems registered, MoUs executed. The MERL framework tracks whether institutions exist, not whether redress and accountability commitments function for the people they protect.	Add outcome-level indicators to the MERL Matrix: complaints received and resolved, average time to resolution against statutory timelines, and discrimination or rights-harm incidents identified and remedied, reported annually alongside existing institutional key performance indicators.	The AU Strategy's redress-and-remedy language commits to an outcome, not the existence of a form. A framework that measures institutions but not whether complaints are resolved does not show whether oversight is working.
14.	Section 4.5.4(2), Core Elements of the AI and other Emerging Technologies Legislative Framework	The Policy commits the future Governance Act to "mandatory AI impact assessments for high-risk systems," without defining what these must cover. The principal pre-deployment assessment tool elsewhere in Kenya's legal framework is the Data Protection Impact Assessment	Define "AI impact assessment" in the Governance Act to require assessment of discrimination, exclusion and other rights harms specifically, not only personal data risk, so that it is not limited to data protection risks alone.	The AU Strategy points to UNESCO's Ethical Impact Assessment as a useful reference model for evaluating AI systems. The UNESCO Recommendation likewise encourages impact assessments that examine broader ethical, human rights and societal effects, including discrimination,

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA)				
S/No	**Section of the Policy**	**Provisions of the Policy**	**Proposed Amendment**	**Rationale for Amendment Recommendation**
		(DPIA) under the Data Protection Act, 2019.		exclusion and environmental impacts, rather than focusing solely on personal data protection. Kenya's own experience with the 2025 Worldcoin case, in which the High Court found unlawful processing of sensitive biometric data, illustrates the value of scrutiny before large-scale deployment, while also showing that data-protection review alone did not capture the broader societal and rights impacts at stake
15.	Section 1.6 (Guiding Principles), Principle 7 — Inclusion and Equity	The provisions reviewed do not name technology-facilitated gender-based violence, deepfakes or AI-enabled harassment as a category requiring specific safeguards.	Require gender impact assessments for high-risk systems, alongside human rights impact assessments, and require platforms to take reasonable steps where recommender or content curation systems amplify AI-generated harassment or non-consensual synthetic media (including deepfakes).	The AU Strategy calls for AI governance to address disproportionate risks to women and marginalised groups. CIPESA's regional research documents AI-enabled gendered harassment as a growing barrier to women's participation online. Generative AI increases this risk by making abusive, synthetic content easier to create and distribute.
16	Section 3.6.1, Data Ecosystem Standards; Section 3.7.4(4), Inclusion of Local Languages	The Policy commits to promoting the inclusion of local languages in "systems affecting public access and service delivery," but does not extend this obligation to the AI-based content-moderation and recommendation systems operated by the major platforms	Extend the local language and inclusive design obligations in Section 3.7.4 to content moderation and recommender systems operating in Kenya, and require platforms registering under the National AI Registry to report	Our research finds AI-based content moderation is largely built for the Global North and struggles with low-resource African languages, forcing over 90% of Africans to switch to a dominant or colonial-era language to use major platforms. Without an explicit obligation,

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA)				
S/No	**Section of the Policy**	**Provisions of the Policy**	**Proposed Amendment**	**Rationale for Amendment Recommendation**
		Kenyans actually use daily.	on Kiswahili and local language content moderation accuracy and human review capacity.	Kenya's most linguistically diverse and rural populations remain the least protected by, and least able to appeal, automated moderation decisions.
17	Section 3.9, Sovereignty and Strategic Autonomy; Section 3.8, Infrastructure and Digital Readiness	The Policy addresses infrastructure and sovereignty in general terms but does not set out how Kenya will address its position within Africa's severe compute deficit.	Direct the National AI and other Emerging Technologies Council to pursue regional compute-sharing and co-investment arrangements under the AU Continental AI Strategy and Smart Africa's implementation structures, and to report annually on Kenya's compute capacity relative to regional peers.	Africa accounts for only around 1% of global compute capacity, constraining the continent's ability to train, fine-tune or evaluate models locally and cheaply. It is essential to close this compute gap. Regional pooling, rather than each country building in isolation, is the more realistic path within Kenya's fiscal constraints.
18	Section 4.6, Funding Arrangements; Section 3.9, Sovereignty and Strategic Autonomy	The Policy's funding arrangements focus on government budgetary allocation, development partner support and public-private partnerships, but do not reference Kenya's existing tax instruments for capturing value from non-resident AI and digital service providers.	Cross-reference the Significant Economic Presence Tax (SEPT) regime, which already extends to "AI and digital assets" income earned by non-resident providers from Kenyan users, in the Policy's funding and sovereignty provisions, and direct the National Treasury and the Council to jointly assess whether SEPT revenue attributable to AI services should be	Kenya's 2025 SEPT regulations already deem non-resident digital service income taxable, at an effective 3% of gross turnover, explicitly extending to AI and digital asset income, and collections from foreign digital companies more than doubled in FY2025/26.[4] This legislated mechanism could ensure foreign AI firms operating in Kenya contribute to the institutions meant to oversee them, and for addressing the data extractivism concerns the Policy elsewhere gestures toward without naming a remedy.

[4] https://www.grantthornton.co.za/insights2/significant-economic-presence-tax/; https://kenyanwallstreet.com/kenyas-digital-tax-2026

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA)				
S/No	**Section of the Policy**	**Provisions of the Policy**	**Proposed Amendment**	**Rationale for Amendment Recommendation**
			ring-fenced, in part, for AI capacity-building and oversight institutions.	
19	Section 3.6.2, Data Frameworks; Section 3.7.6(4), Safeguards for Biometric Identification	The Policy commits to "safeguards" for AI-enabled biometric identification generally, without naming the specific consent, retention and vendor due diligence standard that should apply where private biometric collection intersects with public digital identity infrastructure.	Require that any biometric data collection scheme intersecting with, or seeking future integration into, national digital identity infrastructure obtain prior authorisation from the Office of the Data Protection Commissioner (ODPC) and the National AI and other Emerging Technologies Council, with published findings, before deployment.	The 2025 High Court ruling that the Worldcoin iris-scanning project was unlawfully deployed in Kenya, for want of adequate consent and transparent processing of sensitive biometric data, is the kind of harm a general "safeguards" clause is meant to prevent. This gives the Council and the ODPC a concrete pre-deployment checkpoint rather than a reactive, after-the-harm posture.
20	Section 3.3, Capacity and Human Capital Development	The Policy's capacity building provisions focus on training pipelines, including education integration, teacher capacity, and public sector upskilling, but do not address retention of the AI talent Kenya trains.	Add a policy statement under Section 3.3 committing to retention incentives for Kenyan AI researchers and engineers, including competitive public-research fellowships, tax incentives for domestic AI employers, and diaspora engagement mechanisms to channel skills and investment back into the local ecosystem.	Regional research warns that African AI postgraduates are around 10 times more likely to take up work in the Global North than locally, given better pay and infrastructure, a dynamic that could hollow out the institutions this Policy depends on for oversight and innovation capacity.[5] A training-only strategy risks producing skilled graduates for export rather than local capability.

[5] CIPESA, State of Internet Freedom in Africa 2025

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA)				
S/No	**Section of the Policy**	**Provisions of the Policy**	**Proposed Amendment**	**Rationale for Amendment Recommendation**
21	Section 2.6, Role of County Governments; Section 4.3.2, County AI and Data Readiness Framework	The Policy establishes a County AI and Data Readiness Framework and County AI and Data Readiness Grants, but does not set differentiated targets or minimum-capacity baselines reflecting the wide disparity in county-level digital readiness.	Require the County AI and Data Readiness Framework to publish county-disaggregated baseline indicators for connectivity, device access and digital literacy, and to weight grant allocation toward counties furthest below the national baseline, rather than distributing support uniformly or on a purely competitive basis.	Regional data shows persistent rural-urban and gender gaps in connectivity, and Kenya's own high national averages, including its global lead in ChatGPT adoption at 42.1% of internet users, mask significant disparity between urban and rural, and male and female, users. Without disaggregated targets, county grants risk reinforcing existing advantages rather than closing the gap the framework is meant to address.
22	Section 1.7, Structure of Policy; Section 4.5.3, Key Legislative Proposals	The Policy commits to a future AI Governance Act to be drafted within six months and enacted within 12 months, while there is an AI Bill already before Parliament.	Clarify the relationship between the Policy's proposed AI Governance Act and the AI Bill already tabled in Parliament, including which instrument takes precedence, how the two processes will be reconciled, and a single public timeline covering both.	The AI Bill already in Parliament is a separate legislation from the Policy's own AI Governance Act commitment. Two unreconciled legislative vehicles addressing the same subject matter risk duplication and implementation confusion that has affected other Kenyan digital policy instruments. The Policy should name and resolve this risk rather than leave it to be discovered downstream.