West Africa School on Internet Governance

WAIGF 26

FINAL REPORT

Residential Workshop held in Freetown, Sierra Leone, 11-12 May 2026, as part of the West Africa Internet Governance Forum 2026

www.waigf.ecowas.int 11-15 May 2026 Freetown, Sierra Leone

Contents

EXECUTIVE SUMMARY

The West Africa School on Internet Governance 2026 was implemented as a strategic regional capacity development initiative within the broader West Africa Internet Governance Forum 2026 process. Convened in Freetown, Sierra Leone, on 11 and 12 May 2026, the residential workshop constituted the final applied stage of a wider learning pathway that began with open regional mobilisation, continued through online training, and culminated in policy clinics, peer learning, and structured engagement among fellows, observers, facilitators, and institutional partners. The School was therefore not a stand-alone training event. It was a deliberate investment in the human, institutional, and diplomatic capacities required for West Africa to engage digital transformation as a matter of development, sovereignty, security, rights, and regional integration.

The strategic relevance of the School derives from the accelerating convergence of digital policy issues across West Africa. The region is experiencing fast growth in mobile connectivity, digital financial services, platform economies, data-intensive public services, AI-enabled applications, and cross-border digital markets. At the same time, policy frameworks remain uneven, institutional capacities differ across Member States, and many governance challenges increasingly exceed national borders. Cyber incidents, online harms, remote digital services, data transfers, platform taxation, AI procurement, and interoperable public digital infrastructure cannot be governed effectively through isolated national responses. The School responded directly to this context by strengthening the ability of fellows to analyse complex governance questions, negotiate policy choices, articulate regional positions, and translate multistakeholder dialogue into actionable recommendations.

The 2026 edition was aligned with the WAIGF 2026 strategic context and with the central theme of digital sovereignty and economic value in West Africa's integrated digital market. The discussions moved beyond sovereignty as a narrow notion of territorial control and reframed it as institutional capability, regional coordination, public-interest infrastructure, accountable markets, trusted data governance, rights protection, and strategic participation in global Internet governance. This framing is important for ECOWAS Member States, the African Union, the United Nations system, ICANN, the Internet Society, and development partners because it connects capacity development with the operational requirements of regional digital transformation.

Participation data confirms both the scale of demand and the selectivity of the process. More than 600 applications or expressions of interest were received for the School. A quality-controlled scorecard retained 540 complete source records for detailed analysis, of which 514 were identified as West African and 497 were retained after eligibility filters. A scored pool of 445 applications was assessed against criteria relating to professional relevance, leadership potential, motivation, thematic alignment, regional perspective and diversity contribution.

From this process, 177 participants were selected for the online phase, 150 successfully completed the Internet Society online programme and 30 fellows were selected to attend the residential workshop in Freetown, accompanied by 14 observers. This pathway demonstrates a structured progression from broad regional outreach to rigorous online learning and finally to applied residential policy work.

The composition of the cohort reflected the multistakeholder character of Internet governance. Participants brought perspectives from government and public institutions, civil society, academia, the private sector, media, the technical community and regional policy networks. The online selection pathway represented West African countries and balanced language communities across English and French, while also advancing gender inclusion in comparison with the initial applicant pool. This diversity was central to the learning environment because the programme required fellows to work across disciplines, national contexts and institutional mandates. It also reinforced the principle that digital governance cannot be reduced to technical administration or state regulation alone, but must be shaped through structured cooperation among public authorities, rights advocates, innovators, researchers, technical operators and users.

The residential workshop combined masterclasses, seminars, technical briefings, policy clinics, team drafting, stakeholder mapping, presentations and peer review. Day 1 established the conceptual foundations of Internet governance, the WAIGF architecture and the strategic context of digital sovereignty in West Africa. It examined platform accountability, taxation and regulatory cooperation, before turning to data governance, artificial intelligence governance and redress mechanisms. Day 2 consolidated the first day through peer reflection and focused on the regional digital single market, infrastructure sovereignty, interoperability, cybersecurity cooperation, lawful access and digital trust frameworks. The final practicum required fellows to translate the discussions into four policy briefs addressing platform accountability and fiscal justice, AI-enabled public services and redress, interoperable digital public infrastructure, and regional cyber resilience.

The policy clinic emerged as one of the most consequential components of the School. It exposed fellows to the discipline of policy drafting, stakeholder mapping, negotiation, and concise institutional presentation under time constraints similar to those found in regional and international forums. The four group outputs collectively show that fellows were able to move from conceptual discussion to practical policy architecture. Their briefs proposed a regional framework for digital revenue transparency and consumer protection, rights-based safeguards for AI-enabled public services, an interoperable payment and digital identity corridor, and a 72-hour regional cyber response framework. These outputs are included in annex to this report as evidence of the applied policy value generated by the School. The major outcome of the School was the development of a regional community of practice equipped to engage Internet governance as a multidimensional public policy agenda. Fellows strengthened their understanding of the Internet governance ecosystem, developed analytical capacity around digital sovereignty, built practical familiarity with multistakeholder processes, and produced policy-oriented outputs that can inform national and regional dialogue.

The School also demonstrated the continuing need for systematic investment in capacity development across West Africa, including deeper support for national Schools on Internet Governance, cross-border alumni networks, policy labs, mentorship pathways and structured engagement with ECOWAS, the African Union, the United Nations system, ICANN, the Internet Society and technical community institutions.

This report concludes that WASIG 2026 should be sustained and scaled as a regional leadership platform for Internet governance. The initiative provides a practical model for connecting online learning, residential policy work, regional dialogue and institutional follow-up. It contributes to the development of future negotiators, regulators, researchers, civil society leaders, technical-community actors and public servants capable of advancing an open, secure, inclusive and economically meaningful digital future for West Africa.

Indicator	Value and Interpretation
Public demand	More than 600 applications or expressions of interest were received during the call for participation. A quality-controlled scorecard retained 540 complete source records for detailed analysis.
Regional eligibility	514 source records were identified as West African, and 497 applications were retained after regional eligibility and first-time participation filters.
Scored pool	445 eligible applications were scored through a criteria-based process assessing relevance, leadership potential, motivation, thematic alignment, regional perspective and diversity contribution.
Online learning cohort	177 participants were selected for the online phase delivered through the Internet Society online learning pathway.
Online completion	150 participants successfully completed the online programme, demonstrating strong retention and readiness for advanced policy engagement.
Residential fellowship	30 fellows were selected for the Freetown residential workshop, accompanied by 14 observers and supported by resource persons, facilitators and institutional partners.
Regional coverage	The fellowship pathway represented the countries of West Africa and was designed to sustain bilingual and cross-border policy dialogue across the region.

Strategic Rationale

Internet governance in West Africa has entered a period in which technical connectivity, economic integration, rights protection, cybersecurity, and public-sector digital transformation can no longer be addressed as separate policy agendas. National strategies are increasingly shaped by the same underlying dependencies: resilient infrastructure, trusted data systems, interoperable services, secure networks, accountable digital markets, and institutions capable of coordinating across borders. The value of the Internet for development depends not only on access, but also on the governance arrangements that determine who benefits, who is protected, who participates, and how public value is generated within digital markets.

The region has made significant progress in expanding digital connectivity and strengthening institutional awareness of Internet governance. National Internet Governance Forums, digital transformation strategies, data protection authorities, cybersecurity policies, and innovation ecosystems have emerged across Member States. Nevertheless, disparities in institutional capacity, regulatory maturity, and technical infrastructure remain substantial. These disparities affect the region's ability to negotiate with global platforms, secure critical information infrastructure, govern cross-border data flows, protect users, support startups, and develop trusted public digital infrastructure.

The policy environment is also being reshaped by the growth of artificial intelligence, data-intensive public services, digital identity systems, online financial services, e-commerce platforms, digital advertising, content creation and online betting. These developments generate new economic opportunities but also create governance risks. Revenue generated by digital platforms may be difficult to trace. Automated decision-making may affect rights and access to public services. Cyberattacks may disrupt services beyond national borders. Content moderation systems may fail to understand local languages and social context. Public authorities may become dependent on proprietary cloud or AI vendors without sufficient safeguards. These issues require regional capacity, not only national awareness.

The 2026 West Africa School on Internet Governance was designed to respond to this strategic context. It placed capacity development at the centre of regional digital governance. By bringing together fellows from across the region and exposing them to both conceptual and practical learning, the School contributed to the formation of a West African policy community able to engage with digital sovereignty, cybersecurity, AI governance, infrastructure resilience, platform accountability and digital rights through an integrated lens.

The School was held as part of the West Africa Internet Governance Forum 2026 process in Freetown, Sierra Leone. Its residential component preceded the Youth IGF and the main regional forum, thereby positioning the fellows as active contributors to the broader WAIGF ecosystem rather than passive beneficiaries.

This sequencing strengthened the link between training and policy dialogue. Fellows were prepared not only to understand Internet governance issues, but also to participate in regional discussions with greater confidence, clarity and institutional awareness.

The theme of digital sovereignty and economic value in West Africa's integrated digital market provided the central narrative for the workshop. The discussions deliberately avoided a restrictive interpretation of sovereignty. Instead, sovereignty was approached as the ability of societies and institutions to make informed decisions about digital infrastructure, data, platforms, standards, security and markets while remaining connected to the global Internet. This approach is particularly relevant for West Africa, where regional integration can increase bargaining power, reduce fragmentation and create the trust needed for cross-border digital services.

The rationale behind WASIG 2026, therefore, rested on three strategic considerations. First, the digital transformation of West Africa requires a new generation of leaders who understand the Internet as a governance ecosystem rather than as a narrow technical tool. Second, regional integration cannot be achieved without shared standards, interoperable systems and trusted institutions. Third, the global governance of emerging technologies requires West African actors who can contribute with evidence, clarity and regional perspective to international processes. The School addressed these considerations through a blended pathway combining online learning, residential engagement and policy production.

The workshop also reflected a broader institutional lesson. Digital transformation programmes often focus on infrastructure deployment, legal reform or innovation financing. These areas are essential, but they are insufficient without sustained human capacity. Institutions need individuals who can connect technical questions to public policy, translate rights principles into operational safeguards, design regional coordination mechanisms, and communicate complex issues to decision-makers. WASIG 2026 treated capacity development as a strategic infrastructure for governance itself.

Programme Architecture

The West Africa School on Internet Governance operates within the broader architecture of the West Africa Internet Governance Forum and contributes to the regional implementation of the multistakeholder model. Its institutional role is to prepare participants to understand and engage the policy questions that shape the development and use of the Internet in West Africa. The 2026 residential workshop was anchored in the WAIGF process and supported by a programme design that linked capacity-building, stakeholder dialogue, policy analysis and regional cooperation.

The Freetown edition drew on institutional participation from the host government, the West Africa IGF Secretariat, WASIG coordination and resource persons from the technical community, civil

society, innovation, and Internet governance networks. The opening ceremony, featuring the Ministry of Communication, Technology, and Innovation of Sierra Leone, placed the School within the national and regional public policy context. The presence of facilitators from the WAIGF Secretariat, Jokkolabs Banjul, AFRINIC, and the Internet Society Nigeria Chapter reinforced the multistakeholder nature of the learning environment.

The programme architecture was designed to move from foundations to application. The first day established the conceptual and strategic frame through sessions on the Internet governance ecosystem, digital sovereignty, economic value, platform accountability, taxation, data governance, AI governance, and redress. The second day focused on operational governance challenges through sessions on the regional digital single market, infrastructure sovereignty, interoperability, cybersecurity cooperation, lawful access, and digital trust. The practicum transformed these themes into team-based policy briefs and presentations.

This design was important because it mirrored the complexity of real Internet governance processes. Participants were not asked only to absorb information; they were required to analyse problems, identify stakeholders, weigh trade-offs, work across sectors, and produce concise policy proposals. The architecture, therefore, combined knowledge transfer with diplomatic simulation, technical interpretation, and policy drafting. It prepared fellows to participate in national and regional processes where time is limited, evidence is contested, and consensus must be built across divergent interests.

Programme component	Strategic function
Online phase	Established foundational knowledge and ensured that the residential cohort was prepared for advanced applied work.
Residential masterclasses	Provided conceptual depth on Internet governance ecosystems, sovereignty, digital markets, AI, data and cybersecurity.
Interactive seminars	Created space for fellows to test assumptions, compare national experiences and identify regional policy implications.
Policy clinic	Translated learning into group policy briefs, stakeholder mapping and concise presentation practice.
Peer review	Strengthened accountability, clarity, negotiation discipline and the capacity to defend policy choices.
WAIGF linkage	Connected fellows to the regional forum process and reinforced the continuity between capacity development and regional dialogue.
Session or function	**Resource persons and institutional roles**
Opening Ceremony	Mr. James Cobba, Director of Policy Planning and Tech Compliance, Ministry of Communication, Technology and Innovation, Sierra Leone; Emmanuel Elolo Agbenonwossi, Coordinator, West Africa IGF Secretariat; Folaranmi Umoru, West Africa School on Internet Governance Coordinator
Session 1	Emmanuel Elolo Agbenonwossi, Coordinator, West Africa IGF Secretariat
Session 2	Poncelet Ileleji, CEO, Jokkolabs Banjul
Session 3	Emmanuel Elolo Agbenonwossi, Coordinator, West Africa IGF Secretariat

Session 4	Ms. Nnenna Nwakanma, Tech Advocacy and Cooperation Strategist
Practicum and mentor clinic	Emmanuel Elolo Agbenonwossi; Folaranmi Umoru; Poncelet Ileleji; Behou Brice Abba, Community Development Manager, AFRINIC; Engr. Kunle Olorundare, President, Internet Society Nigeria Chapter

Methodology and Pedagogical Approach

The methodology of WASIG 2026 was built around a blended learning model. The online phase provided a broad regional entry point and introduced core Internet governance concepts through the Internet Society online learning pathway. The residential phase then functioned as an intensive policy laboratory in which selected fellows applied their learning to regional scenarios. This sequencing increased the quality of residential engagement because participants entered the workshop with a common baseline of knowledge and a demonstrated record of completion.

The pedagogical approach combined masterclass delivery, facilitated dialogue, practical assignments, peer learning, team-based drafting and simulated policy presentation. The masterclasses provided structured knowledge. The facilitated dialogues encouraged participants to compare national and sectoral experiences. The policy clinic required teams to convert thematic knowledge into concrete policy options. Peer review made participants accountable to one another and exposed them to the discipline of concise institutional communication.

The residential workshop placed particular emphasis on applied policy reasoning. Each group was required to analyse a governance problem, map stakeholders, identify risks, propose options and prepare a short presentation. This approach reflected the realities of regional and international policy processes, where actors must often present complex ideas in limited time and where the ability to frame trade-offs is as important as technical knowledge. Fellows were encouraged to distinguish between what should be harmonised at regional level and what should remain within national discretion.

The use of policy briefs as final outputs was a deliberate pedagogical choice. Policy briefs require clarity, prioritisation and evidence-based recommendation. They also force participants to move beyond broad principles toward institutional feasibility. In the context of West Africa, where digital governance challenges require coordination among governments, regulators, the technical community, civil society, private-sector actors and development partners, the ability to produce concise, actionable policy documents is a core leadership skill.

The School also used peer interaction as a learning tool. Fellows were placed in mixed teams to ensure that group discussions brought together different countries, languages, sectors and professional experiences. This created a practical simulation of multistakeholder governance. Participants had to negotiate terminology, reconcile diverse priorities and produce collective

outputs. In doing so, they developed not only technical understanding but also the interpersonal and diplomatic competencies required for regional cooperation.

The approach was further strengthened by the presence of observers, facilitators and resource persons who provided feedback on substance, presentation, stakeholder mapping and feasibility. The mentor clinic acted as a bridge between theoretical understanding and policy production. It helped participants refine their recommendations, identify missing stakeholders, sharpen problem statements and avoid overly broad or unrealistic policy proposals. This mentoring function is essential for transforming capacity-building into a more mature form of policy readiness.

Learning method	**Contribution to capacity development**
Masterclass	Provided structured exposure to strategic Internet governance concepts and regional policy context.
Seminar discussion	Allowed fellows to interrogate issues through national and sectoral experience.
Technical briefing	Connected policy questions with operational requirements in cybersecurity, infrastructure and lawful access.
Policy clinic	Built capacity in problem definition, stakeholder mapping, prioritisation and institutional drafting.
Team presentation	Developed concise communication, evidence-based argumentation and negotiation discipline.
Peer review	Strengthened accountability, comparative learning and the ability to defend recommendations.

Selection Pipeline and Participant Analysis

The participant pathway demonstrates that WASIG 2026 was implemented as a structured regional pipeline. The call for participation generated more than 600 applications or expressions of interest, confirming strong regional demand for Internet governance capacity development. For data analysis and selection management, the scorecard retained 540 complete source records. Within this set, 514 applications were identified as West African, 497 were retained after eligibility screening, and 445 were scored through a criteria-based process. This filtering process ensured that the online phase and residential fellowship were grounded in merit, relevance, and regional inclusion.

The official online learning cohort comprised 177 selected participants. Of these, 150 completed the Internet Society online programme. The residential phase in Freetown brought together 30 fellows, accompanied by 14 observers. The final cohort represented the countries of West Africa and was designed to enable cross-border learning across linguistic, institutional, and professional communities. The selection ratios also indicate a meaningful level of competitiveness. The residential cohort represented a highly selected group emerging from a broad regional pool and a completed online pathway.

The selection approach combined quality and inclusion. The scorecard assessed applicants against professional relevance, leadership potential, motivation quality, thematic alignment, regional perspective, and diversity contribution. This model is appropriate for an Internet governance school because the desired outcome is not only individual knowledge gain. The programme seeks to identify participants who can contribute to national and regional ecosystems, facilitate dialogue, produce policy insights and remain active after the training. The selection process therefore treated the fellowship as a leadership investment.

Gender and language considerations were incorporated into the selection pathway. Analysis of the data indicates that women represented a higher share of the named online selection list than of the eligible applicant pool, demonstrating an intentional movement toward gender balance. The online cohort also maintained English and French language representation, an important factor for West Africa's regional governance ecosystem. Future editions should continue strengthening multilingual access, including Portuguese-language support and mechanisms that enable participants from smaller applicant pools to remain visible within the regional community.

Stakeholder diversity was equally important. The fellows and online participants reflected government, civil society, academia, the private sector, the technical community, media and policy networks. This composition is directly aligned with the multistakeholder model. It also increased the practical relevance of the workshop because participants brought different assumptions about regulation, rights, innovation, infrastructure and public service delivery. The value of the residential phase came in part from requiring these perspectives to interact in real time around common regional scenarios.

The thematic interests expressed in the application pipeline closely matched the workshop agenda. AI governance, data protection, cybersecurity and regional cooperation appeared as prominent areas of interest among applicants. This alignment reinforces the policy relevance of the School. It shows that fellows entered the programme with demand for precisely the issues that now define West Africa's digital governance agenda: responsible AI, trusted data ecosystems, cybersecurity resilience, platform accountability and regional interoperability.

Pipeline stage	Figure	Interpretation
Applications and expressions of interest	More than 600	Provided structured exposure to strategic Internet governance concepts and regional policy context.
Complete records retained for analysis	540	Quality-controlled source records used for selection management and statistical review.
West African records	514	The application pool was overwhelmingly regionally relevant.
Eligible applications	497	Applications retained after regional eligibility and first-time participation filters.
Scored applications	445	Applications reviewed through a criteria-based scorecard.
Peer review	177	Participants admitted to the Internet Society online learning stage.

Pipeline stage	Figure	Interpretation
Graduated from online programme	150	Participants who completed the online learning pathway.
Residential fellows in Freetown	30	Final cohort selected for intensive applied policy work.
Observers	14	Additional participants supporting dialogue, observation and institutional learning.

Dimension	Analytical observation
Regional representation	The selection pathway represented West African countries and was designed to mitigate concentration in larger applicant markets.
Gender inclusion	The programme moved toward stronger gender balance compared with the eligible applicant pool.
Technical briefing	The online selection reflected English and French communities, while future editions should further support Portuguese inclusion.
Policy clinic	Built capacity in problem definition, stakeholder mapping, prioritisation and institutional drafting.
Team presentation	Developed concise communication, evidence-based argumentation and negotiation discipline.
Peer review	Strengthened accountability, comparative learning and the ability to defend recommendations.

Detailed Coverage of the Residential Workshop

The residential workshop was structured over two days and followed a progression from foundational understanding to applied regional policy work. The programme combined ceremony, masterclass, seminar, technical briefing, practicum, mentoring, peer review and closing synthesis. The sequence allowed fellows to situate Internet governance within both the global multistakeholder system and the specific regional context of West Africa.

Date	Component	Substantive focus
11 May	Opening and orientation	Registration, participant onboarding and opening ceremony with the Ministry of Communication, Technology and Innovation of Sierra Leone, WAIGF Secretariat and WASIG coordination.
11 May	Session 1	Internet governance ecosystem, WAIGF architecture and the 2026 strategic context.
11 May	Session 2	Digital sovereignty and economic value in West Africa's integrated digital market.
11 May	Session 3	Platform accountability, taxation and regulatory cooperation.
11 May	Session 4	Data governance, artificial intelligence governance and redress mechanisms.
11 May	Practicum	Team formation, policy clinic briefing and deliverables orientation.
12 May	Recap	Peer reflection and consolidation of the first day.
12 May	Session 5	Regional digital single market, infrastructure sovereignty and interoperability.
12 May	Session 6	Cybersecurity cooperation, lawful access and digital trust frameworks.
12 May	Mentor clinic	Policy briefs, stakeholder mapping, team drafting and presentation rehearsal.
12 May	Presentations	Team presentations, peer review, synthesis of policy outputs and closing ceremony.

Policy Clinic and Group Outputs

The policy clinic was the central applied component of the residential workshop. It required the fellows to develop practical policy briefs around selected regional challenges. The outputs demonstrate that the School generated concrete analytical products and not only participant exposure. The four group briefs are included in annex and are synthesised below for institutional use.

Group	Policy focus	Core recommendations
Group 1	Platform accountability and fiscal justice, with online betting platforms as a case study	Regional digital revenue transparency, stronger consumer and youth protection, and co-regulatory dialogue among governments, platforms, regulators, telecoms, fintechs and civil society.
Group 2	Data, AI and redress mechanisms for AI-enabled public services	National AI governance standards, stronger procurement governance, AI impact assessments, bias testing, independent oversight, human review and accessible remedies.
Group 3	Digital single market and interoperable public infrastructure	A regional corridor for payments and digital identity, harmonised trust layers and national discretion over foundational registries and local implementation.
Group 4	ECOWAS cyber resilience and a 72-hour regional response framework	National CERT/SOC capacity, ECOWAS cyber coordination, shared incident playbook, harmonised digital evidence rules and multilingual crisis communication.

Group 1. Platform accountability and fiscal justice

Group 1 addressed the economic and regulatory challenges created by online betting, digital advertising and cross-border platform activity. The brief correctly identifies that online betting platforms operate across jurisdictions, rely on mobile penetration and mobile money ecosystems, and create both revenue opportunities and consumer protection risks. The group's analysis is policy-relevant because it links platform accountability with fiscal transparency, youth protection and regulatory cooperation.

The policy significance of the brief lies in its recognition that national responses are often fragmented. A platform may serve users in multiple ECOWAS Member States while reporting revenues, taxes or operational data in ways that are difficult for individual governments to verify. This creates risks for fiscal fairness and for public trust in digital markets. A regional transparency framework would enable Member States to coordinate reporting expectations, reduce arbitrage and build a stronger evidence base for digital taxation.

The group's recommendation for co-regulation is particularly important. Platform governance should not be designed as a binary choice between prohibition and market freedom. A balanced approach can require transparency and consumer protection while preserving innovation. The recommended involvement of telecom operators and fintechs is also practical because payment rails and digital advertising channels often provide critical information for traceability and risk management.

Group 2. Data, AI and redress mechanisms

Group 2 examined the deployment of AI-enabled public services involving cross-border data hosting and algorithmic decision support. The brief identifies a wide range of risks, including algorithmic bias, lack of transparency, privacy breaches, cross-border data risks, cybersecurity attacks, child data misuse, weak accountability, vendor lock-in and poor procurement governance. This reflects a mature understanding of AI governance as an institutional issue rather than a narrow technical question.

The recommended rights-based and citizen-centred approach is directly relevant for governments considering AI in service delivery. Public-sector AI systems can affect access to benefits, identity, health, education, employment and security. Where such systems are not transparent or contestable, they can undermine public trust and generate rights violations. The group's emphasis on human oversight, appeal mechanisms and clear complaint procedures is therefore essential.

The brief also identifies procurement as a strategic control point. Governments should require AI impact assessments, bias testing, vendor accountability provisions and data sovereignty protections before deployment. This is an area where regional guidance could be valuable, especially for smaller administrations that may lack in-house technical expertise. ECOWAS and development partners could support model procurement clauses, audit tools and peer learning for AI-enabled public services.

Group 3. Digital single market and interoperable public

Group 3 produced a policy note on a corridor involving Guinea, Sierra Leone and Senegal for interoperable payments and digital identity. The brief's core insight is that interoperability is not simply a technical engineering problem. It is a matter of governance, trust and public interest. This framing is strategically important because many digital integration initiatives fail when they focus on systems integration without addressing liability, consumer protection, data protection and institutional accountability.

The brief proposes a phased roadmap from political alignment and institutional framing to architecture, pilot deployment, regulated market opening and regional institutionalisation. This sequencing is credible because it recognises that trust frameworks must be established before cross-border services can scale. It also distinguishes between regional layers that should be harmonised and national layers that should remain differentiated. This distinction is essential to preserving sovereignty while enabling integration.

The layers proposed for harmonisation include identity trust frameworks, technical standards and APIs, minimum data schemas, cybersecurity rules, routing systems, certification, consumer

protection, procurement rules, cloud portability and common reporting. The layers left to national discretion include civil registry architecture, enrolment modalities, user experience, languages and internal institutional organisation. This balance should inform future ECOWAS work on the digital single market and public digital infrastructure.

Group 4. ECOWAS cyber resilience and a 72-hour regional

Group 4 addressed cyber resilience through a proposed 72-hour regional response framework. The brief recognises that the digital economy of West Africa increasingly depends on interconnected payment systems, customs platforms, digital identity systems and government networks. A cyber incident in one Member State can rapidly affect confidence and services across borders. The group therefore frames cyber resilience as a governance, communication and legal cooperation issue, not only as a technical function.

The recommendations are operationally relevant. The group calls for stronger national CERTs and SOCs, 24/7 incident response capacity, alignment of cybercrime and digital evidence laws, national crisis communication systems linked regionally, cybersecurity skills development and an ECOWAS Cyber Coordination Centre. It also proposes a shared incident playbook, common response rules, a multilingual crisis template and faster legal cooperation for information and evidence sharing.

The policy value of the brief lies in its emphasis on the first 72 hours of a crisis. During this period, delays in verification, legal process, public communication or technical escalation can amplify harm. A regional framework would help Member States act jointly while protecting sovereignty through controlled information sharing. The recommendation to align cybersecurity measures with privacy safeguards is also critical to maintaining public trust.

Strategic Outcomes and Added Value

WASIG 2026 generated outcomes at individual, institutional and regional levels. At the individual level, fellows strengthened their understanding of Internet governance architecture, digital sovereignty, data and AI governance, platform accountability, cybersecurity and regional integration. They also developed practical skills in policy drafting, stakeholder mapping, concise communication and peer review. These skills are essential for participation in national, regional and global digital policy processes.

At the institutional level, the School created a mechanism for connecting diverse actors around shared policy challenges. Government officials, civil society representatives, academics, private-sector participants, technical community actors and observers engaged the same issues from different perspectives. This interaction increases the possibility of future collaboration because participants leave with shared language, direct relationships and practical awareness of each other's mandates.

At the regional level, the School reinforced the WAIGF process as a capacity-building and policy-development platform. It demonstrated that regional Internet governance forums can produce applied outputs and help prepare stakeholders for more substantive engagement in policy processes. The integration of policy briefs into the School is particularly important because it creates tangible products that can inform follow-up by ECOWAS institutions, national governments, civil society, technical actors and development partners.

The School also produced strategic insight on how West Africa should approach digital sovereignty. Across sessions and policy outputs, fellows converged around the idea that sovereignty is strengthened through shared standards, accountable platforms, interoperable public infrastructure, data protection, AI safeguards, cyber coordination and local expertise. This is a sophisticated and operational understanding of sovereignty that avoids both dependence and isolation.

The initiative added value by connecting the Internet Society online learning pathway with a residential regional policy lab. This blended model can be replicated and scaled. It allows broad outreach across the region, ensures baseline knowledge, rewards completion and concentrates residential resources on participants ready for advanced engagement. For donors and partners, this model offers a credible pathway for measurable capacity development and policy impact.

The School also strengthened regional leadership pipelines. Fellows who completed the programme can contribute to national IGFs, WAIGF, youth forums, regulatory consultations, civil society initiatives, technical community programmes and international processes. The alumni network should therefore be treated as a strategic asset. With structured follow-up, it can support research, policy dialogue, mentorship and implementation across West Africa.

Outcome area	Evidence of added value	Strategic implication
Knowledge acquisition	Online completion by 150 participants and intensive residential learning by 30 fellows.	A common regional knowledge baseline was established.
Policy production	Four group policy briefs on priority regional issues.	The School generated applied outputs that can inform follow-up.
Regional dialogue	Participants and observers engaged across countries, sectors and language communities.	A cross-border community of practice was strengthened.
Leadership development	Fellows practised negotiation, presentation and peer review.	The initiative supports a new generation of digital governance leaders.
Institutional relevance	Themes aligned with **WAIGF 2026** and regional priorities on sovereignty, markets and trust.	The School contributes directly to regional digital policy ecosystems.

Strategic Policy Implications for Institutions and Partners

The strategic importance of WASIG 2026 extends beyond the delivery of a successful residential workshop. The School provides evidence of a regional model through which capacity development, policy dialogue and institutional cooperation can reinforce one another. The implications are relevant for ECOWAS, the African Union, the United Nations system, ICANN, the Internet Society, development partners and national governments because the digital governance challenges discussed in Freetown correspond directly to regional and global policy agendas.

Implications for ECOWAS and regional integration

For ECOWAS, the School confirms that regional digital integration requires a human capacity layer in addition to legal instruments and infrastructure initiatives. A digital single market cannot function on the basis of technical interoperability alone. It requires officials, regulators, private-sector actors, civil society leaders and technical experts who understand common trust frameworks, consumer protection, cybersecurity baselines, cross-border data governance and the political economy of digital markets.

The policy clinic outputs are particularly relevant for ECOWAS because they translate regional priorities into operational proposals. The Group 3 corridor for payments and digital identity illustrates how integration can be phased while respecting national sovereignty. The Group 4 cyber resilience framework demonstrates how regional coordination can reduce the first 72-hour response gap during cyber incidents. Group 1 and Group 2 show how digital taxation, platform accountability and AI procurement require frameworks that are coherent across jurisdictions.

The implication is that ECOWAS could use WASIG as a structured feeder into regional policy processes. Alumni and policy briefs can support consultations, working groups and regional model guidance. This would enhance the legitimacy of regional digital policy by connecting it to a trained community of practitioners from multiple stakeholder groups and countries.

Implications for the African Union digital agenda

For the African Union, WASIG 2026 contributes to the continental objective of strengthening African participation in digital governance, cybersecurity, data governance and emerging technology policy. The School demonstrates that continental frameworks require regional translation and local capacity to become effective. West Africa's experience can inform broader continental efforts to align digital transformation with sovereignty, inclusion and rights. The workshop discussions also resonate with continental debates on data governance, AI governance, digital public infrastructure and cyber resilience. Participants recognised that African digital sovereignty depends on the ability to negotiate data partnerships, assess technology procurement, build interoperable infrastructure

and participate in standards processes. These are areas where regional Schools on Internet Governance can function as implementation partners for continental policy agendas.

The African Union and regional economic communities could jointly support a networked model of digital governance schools. Such a model would allow regional adaptation while enabling cross-regional learning, policy comparison and a stronger African voice in global Internet governance processes.

Implications for the United Nations system and digital cooperation

For the United Nations system, the School reflects the continuing importance of inclusive and multistakeholder capacity development in achieving digital cooperation objectives. The issues addressed in Freetown are directly linked to development, peace and security, human rights, economic transformation and institutional resilience. AI governance, cybersecurity, digital rights and public digital infrastructure are now core development questions rather than specialised technology topics.

WASIG 2026 also demonstrates the value of regional forums as spaces where global principles can be translated into practical policy reasoning. Participants did not only discuss abstract norms; they considered procurement clauses, incident playbooks, redress channels, interoperability layers and platform transparency. This operational orientation is important for UN agencies seeking to support implementation at national and regional levels.

The United Nations system could support WASIG through expertise, policy toolkits, youth leadership programmes, digital rights guidance, AI governance resources, cyber capacity-building and monitoring frameworks. Such support would reinforce the principle that meaningful digital cooperation depends on informed participation from all regions and stakeholder groups.

Implications for ICANN, the Internet Society and the technical community

For ICANN, the Internet Society and the broader technical community, WASIG 2026 reinforces the need to bridge technical Internet governance and public policy. Fellows engaged issues of naming, numbering, infrastructure, security, access, standards and interoperability through a broader governance lens. This is essential because many public policy debates about sovereignty, security and platforms are shaped by assumptions about Internet architecture that may not always be technically accurate.

Technical community involvement helps ensure that policy debates remain grounded in the principles of openness, interoperability, resilience and security. It also helps policymakers understand operational dependencies. At the same time, the School gives technical actors a clearer view of rights, development, fiscal and institutional concerns. This mutual learning is central to a healthy Internet governance ecosystem.

Sustained engagement could include fellowships, technical briefings, participation in regional network operator groups, domain name system capacity-building, routing security training, measurement projects and mentorship for WASIG alumni. This would strengthen the connection between Internet infrastructure governance and regional policy leadership.

Implications for development partners and donors

For development partners and donors, the School provides a credible platform for investing in capacity development with measurable policy value. The pathway from more than 600 expressions of interest to 177 online selections, 150 graduates and 30 residential fellows demonstrates demand, filtering, completion and intensive application. The production of four policy briefs further shows that the programme can generate outputs that inform institutional dialogue.

Support for WASIG should therefore be designed as multi-year institutional investment rather than event sponsorship. Funding can strengthen curriculum development, translation, accessibility, data systems, alumni coordination, mentorship, policy labs and impact monitoring. It can also help connect fellows to implementation opportunities in their countries and to regional institutions.

The donor value proposition is strong because the School addresses multiple development priorities at once: youth leadership, digital transformation, cybersecurity, responsible AI, inclusion, digital rights, institutional strengthening and regional integration. Investment in WASIG is thus investment in the governance capacity that makes other digital development projects more sustainable.

Implementation Roadmap and Sustainability Framework

The sustainability of WASIG requires a structured pathway that extends beyond the residential workshop. The 2026 edition demonstrated the value of a blended learning and policy clinic model. The next step is to institutionalise follow-up mechanisms so that fellows remain connected to national and regional processes and so that the outputs of the School inform practical policy development.

Phase	Indicative timeframe	Priority actions
Phase 1. Immediate consolidation	0-6 months	Validate the final report, disseminate the Freetown Communiqué, share the policy briefs with institutional partners, establish alumni communication channels and identify country focal points.
Phase 2. Policy translation	6-12 months	Convert group policy briefs into regional discussion notes, organise online policy labs, support fellows to convene national feedback sessions and align outputs with WAIGF and ECOWAS workstreams.
Phase 3. Institutional engagement	12-24 months	Connect alumni to regional consultations, national IGFs, technical community events, AI and cyber policy dialogues, and partner-supported implementation opportunities.
Phase 4. Scaling and renewal	24 months and beyond	Develop a multi-year WASIG programme with recurring online cohorts, annual residential policy clinics, mentorship, research support and impact tracking.

The alumni network should be treated as the central sustainability mechanism. A structured alumni system can maintain contact across countries, support peer learning, identify national opportunities and document contributions to policy processes. Country focal points can help connect fellows with national IGFs, digital policy consultations, youth programmes and technical community initiatives. Regional coordination can ensure that these national activities feed back into WAIGF.

Policy labs should be introduced as a follow-up modality. Each lab could focus on one theme from the residential workshop, such as AI procurement, platform accountability, cyber incident response, digital identity interoperability or data governance. Alumni teams could work with mentors to produce short national or regional policy notes. This would sustain the applied learning model and generate a pipeline of evidence for institutions.

The fellowship model should also include mentorship after the residential phase. Mentors from regional institutions, the technical community, academia, civil society and the private sector can help fellows refine outputs, engage decision-makers and navigate policy processes. Mentorship is especially important for young professionals who have technical competence but limited access to institutional networks.

A multi-year partnership framework would make the School more predictable and effective. Recurring support from partners could cover online platform access, interpretation and translation, travel fellowships, learning materials, data management, facilitator honoraria, research support and alumni activities. Predictable financing would also allow the curriculum to evolve with emerging issues such as generative AI, digital public infrastructure, cloud governance, cyber norms and platform regulation.

Sustainability also depends on documentation. Each edition should produce a report, a communiqué, a recommendations paper, an executive summary and policy briefs. These documents should be used not only for reporting, but also as inputs to policy dialogue. Over time, they can create a regional knowledge archive on West African Internet governance priorities and the evolution of stakeholder perspectives.

Sustainability component	Purpose	Suggested output
Alumni network	Maintain regional community of practice and peer learning.	Country focal points, mailing list, quarterly dialogues.
Policy labs	Translate learning into practical policy notes.	Thematic briefs for national and regional processes.
Mentorship	Support fellows in implementation and institutional engagement.	Mentor matching, clinics and review sessions.
Partner framework	Provide predictable financial and technical support.	Multi-year cooperation plan and annual budget.
Impact documentation	Track outcomes and demonstrate value to partners.	Annual alumni impact report and policy output tracker.

Strategic Recommendations

The recommendations below are designed to translate the lessons of WASIG 2026 into practical follow-up for governments, regional institutions, the technical community, civil society, academia, the private sector and international partners. They are intentionally framed at strategic level because implementation will require adaptation to national mandates and institutional contexts.

Governments and national public institutions

Recommendation 1. Integrate Internet governance capacity development into national digital transformation strategies, including structured participation in national IGFs, regional forums and global policy processes.

Recommendation 2. Develop or update national frameworks for AI governance, data protection, digital public infrastructure, cybersecurity and platform accountability, with clear institutional mandates and rights-based safeguards.

Recommendation 3. Use public procurement as a governance tool by requiring AI impact assessments, data protection clauses, audit rights, cloud portability, vendor accountability and accessible redress mechanisms.

Recommendation 4. Strengthen national CERTs and SOCs, crisis communication systems and incident escalation protocols, while ensuring that cybersecurity measures remain consistent with human rights and due process.

Recommendation 5. Support national alumni chapters and policy labs that can translate WASIG learning into country-level consultations, research notes and stakeholder engagement.

ECOWAS and regional institutions

Recommendation 1. Institutionalise a regional digital governance capacity programme linked to WAIGF, national IGFs and the ECOWAS digital transformation agenda.

Recommendation 2. Develop regional guidance on digital service transparency, digital taxation cooperation, platform accountability and consumer protection for cross-border digital services.

Recommendation 3. Advance a regional trust framework for interoperable digital identity, payments and public digital infrastructure, distinguishing between harmonised regional layers and nationally differentiated implementation layers.

Recommendation 4. Establish or strengthen an ECOWAS cyber coordination mechanism, including a shared incident playbook, multilingual crisis communication templates and rapid legal cooperation channels for digital evidence.

Recommendation 5. Support regional model clauses and policy toolkits for AI procurement, data protection, cloud portability and public-sector algorithmic accountability.

Technical community actors

Recommendation 1. Contribute to capacity development on Internet infrastructure, routing, naming, numbering, cybersecurity, open standards and interoperability in accessible policy language.

Recommendation 2. Support fellows and national institutions in understanding the operational implications of digital public infrastructure, critical information infrastructure protection and cyber incident response.

Recommendation 3. Strengthen engagement between WASIG alumni and regional technical organisations, including network operator groups, research and education networks, national CERTs and standards communities.

Civil society and rights-based organisations

Recommendation 1. Use the WASIG alumni network to strengthen advocacy on digital rights, privacy, online safety, content moderation, platform transparency, gender inclusion and access to remedy.

Recommendation 2. Participate in co-regulatory mechanisms for platform accountability and consumer protection, especially in areas affecting youth, vulnerable groups and linguistic minorities.

Recommendation 3. Support public awareness and civic monitoring of AI-enabled public services, digital identity systems, online harms and cyber crisis communication.

Academia and research institutions

Recommendation 1. Develop research partnerships on West African digital sovereignty, AI governance, cybersecurity cooperation, platform taxation, data governance and interoperability.

Recommendation 2. Integrate Internet governance modules into university programmes in law, computer science, public policy, economics, journalism and international relations.

Recommendation 3. Support evidence generation for WAIGF and ECOWAS policy processes through policy briefs, country case studies, comparative research and evaluation of digital transformation programmes.

Private sector and innovation ecosystem

Recommendation 1. Engage constructively in platform accountability, consumer protection, data protection, cybersecurity and interoperability dialogues, including through transparent reporting and responsible innovation commitments.

Recommendation 2. Support regulatory sandboxes and pilot projects that test cross-border payments, identity, data exchange and digital services under appropriate safeguards.

Recommendation 3. Invest in local talent development, cybersecurity skills, open standards, accessible services and responsible AI practices.

International partners and donors

Recommendation 1. Provide multi-year support for WASIG as a regional capacity development platform rather than funding it as an isolated annual event.

Recommendation 2. Align support with regional priorities on digital sovereignty, public digital infrastructure, cybersecurity resilience, AI governance, digital rights and inclusive digital transformation.

Recommendation 3. Support mentorship, alumni grants, policy labs, translation, accessibility, evidence generation and structured engagement between fellows and institutions such as ECOWAS, AU, ICANN, the Internet Society and United Nations agencies.

Priority action	Lead actors	Suggested horizon
Create a WASIG alumni policy network with country focal points.	WAIGF Secretariat, WASIG coordination, national IGFs	Country focal points, mailing list, quarterly dialogues.
Prepare a regional synthesis of the four policy briefs for WAIGF and ECOWAS consideration.	WASIG coordination, fellows, mentors	Thematic briefs for national and regional processes.
Develop model guidance on AI procurement and redress mechanisms.	ECOWAS, data protection authorities, academia, partners	Mentor matching, clinics and review sessions.
Pilot a regional digital public infrastructure dialogue on identity and payments interoperability.	ECOWAS, central banks, regulators, technical community, private sector	Multi-year cooperation plan and annual budget.
Design a regional cyber incident simulation and response playbook.	ECOWAS, national CERTs, law enforcement, technical partners	Annual alumni impact report and policy output tracker.
Establish annual follow-up policy labs linked to WAIGF.	WAIGF Secretariat, development partners, alumni network	

Conclusion

The West Africa School on Internet Governance Residential Workshop held in Freetown on 11 and 12 May 2026 demonstrated that capacity development is a strategic condition for digital sovereignty, regional integration and inclusive digital transformation. The School connected online learning, rigorous selection, residential engagement, policy drafting and regional dialogue into a coherent capacity-building model. It prepared fellows to engage with the complex governance issues that now shape the digital future of West Africa.

The main institutional lesson is that West Africa's digital governance agenda requires more than laws and infrastructure. It requires people and institutions able to interpret technologies, negotiate policy choices, defend rights, coordinate across borders and build trust among stakeholders. WASIG 2026 contributed directly to this need by strengthening a new generation of Internet governance leaders who can operate across public institutions, civil society, academia, the technical community, the private sector and regional forums.

The workshop also clarified the policy meaning of digital sovereignty for the region. Sovereignty is not isolation from the global Internet. It is the ability to generate public value, protect rights, secure

infrastructure, govern data, hold platforms accountable, adopt responsible AI, coordinate cyber resilience and participate effectively in global governance processes. In West Africa, this ability will be strengthened through regional cooperation and through sustained investment in human capacity.

The continuation of WASIG should therefore be treated as a regional priority. With adequate support, the School can become a standing platform for leadership development, policy innovation, multistakeholder cooperation and institutional follow-up. It can help ensure that the digital transformation of West Africa is not only faster, but also safer, more inclusive, more accountable and more aligned with the development aspirations of the region.

Annex A. Programme Agenda

The following agenda summarises the residential workshop sessions held on 11 and 12 May 2026 in Freetown, Sierra Leone, as part of the WAIGF 2026 process.

Date	Session	Description
11 May	Opening and orientation	Registration, participant onboarding and opening ceremony with the Ministry of Communication, Technology and Innovation of Sierra Leone, WAIGF Secretariat and WASIG coordination.
11 May	Session 1	Internet governance ecosystem, WAIGF architecture and the 2026 strategic context.
11 May	Session 2	Digital sovereignty and economic value in West Africa's integrated digital market.
11 May	Session 3	Platform accountability, taxation and regulatory cooperation.
11 May	Session 4	Data governance, artificial intelligence governance and redress mechanisms.
11 May	Practicum	Team formation, policy clinic briefing and deliverables orientation.
12 May	Recap	Peer reflection and consolidation of the first day.
12 May	Session 5	Regional digital single market, infrastructure sovereignty and interoperability.
12 May	Session 6	Cybersecurity cooperation, lawful access and digital trust frameworks.
12 May	Mentor clinic	Policy briefs, stakeholder mapping, team drafting and presentation rehearsal.
12 May	Presentations	Team presentations, peer review, synthesis of policy outputs and closing ceremony.

Annex B. Participant Statistics and Selection Data

The official reporting figures indicate more than 600 applications or expressions of interest, 177 online selections, 150 online graduates, 30 residential fellows and 14 observers. The detailed scorecard analysis used 540 complete source records and provides the basis for the structured data below.

Indicator	Value and reporting note
Public demand	More than 600 applications or expressions of interest were received during the call for participation. A quality-controlled scorecard retained 540 complete source records for detailed analysis.
Regional eligibility	514 source records were identified as West African and 497 applications were retained after regional eligibility and first-time participation filters.
Scored pool	445 eligible applications were scored through a criteria-based process assessing relevance, leadership potential, motivation, thematic alignment, regional perspective and diversity contribution.
Online learning cohort	177 participants were selected for the online phase delivered through the Internet Society online learning pathway.
Online completion	150 participants successfully completed the online programme, demonstrating strong retention and readiness for advanced policy engagement.
Residential fellowship	30 fellows were selected for the Freetown residential workshop, accompanied by 14 observers and supported by resource persons, facilitators and institutional partners.
Regional coverage	The fellowship pathway represented the countries of West Africa and was designed to sustain bilingual and cross-border policy dialogue across the region.

Participation dimension	Institutional relevance
Online to residential pathway	Demonstrates an efficient blended model in which online completion acts as a gateway to intensive applied learning.
Country representation	Reinforces the School as a regional rather than national initiative and supports the creation of a West African community of practice.
Observer participation	Allows institutions and strategic stakeholders to follow learning outcomes and support continuity.
Stakeholder diversity	Ensures that public policy, technical, private-sector, academic and rights-based perspectives interact during the learning process.
Gender and language inclusion	Strengthens legitimacy and ensures broader access to regional digital policy dialogue.

Annex C. Policy Briefs Produced by the Four Groups

The following annex presents publication-ready versions of the four policy documents produced during the residential policy clinic. The texts preserve the substance of the group outputs while aligning formatting with the institutional style of this report.

Annex C1. Group 1 Policy Brief. Platform Accountability and Fiscal Justice

Case study: Online betting platforms such as 1xBet: The rapid growth of online betting platforms, digital advertising and the creator economy is transforming the digital ecosystem in West Africa. This expansion is accompanied by challenges related to financial transparency, fiscal fairness, consumer protection and regulatory coordination among ECOWAS Member States. In a context of growing cross-border digital transactions, fragmented national responses are insufficient. A coordinated regional approach is required to strengthen digital governance, preserve innovation and promote sustainable African digital sovereignty.

Key findings include difficulty in tracing digital revenue generated by platforms operating across multiple jurisdictions, limited fiscal transparency for national governments, increased exposure of young people to risks associated with online gambling, fragmented regulatory frameworks and a growing need for cooperation among governments, platforms, telecom operators, fintechs, regulators and civil society.

Priority policy options include establishing a regional framework for digital transparency, strengthening consumer protection and promoting co-regulation that fosters innovation. Platform accountability and fiscal fairness are strategic issues for Internet governance in West Africa. A regional, multistakeholder and balanced approach will strengthen digital trust, support innovation and consolidate digital sovereignty.

Stakeholder	Interest	Description
ECOWAS Member States	Fiscal fairness and regulatory stability	Harmonisation of digital policies
Regulatory authorities	Consumer protection	Oversight and compliance
Digital platforms	Growth and market access	Transparency and cooperation
Telecom operators and fintechs	Payment security	Support for transaction traceability
Civil society	Protection of digital rights	Awareness and civic monitoring

Annex C2. Group 2 Policy Brief. Data, AI and Redress Mechanisms

The deployment of AI-enabled public services can improve efficiency, service delivery and decision-making in government. However, automated systems involving cross-border data hosting and algorithmic decision support introduce legal, ethical, operational and governance risks. These include algorithmic bias, lack of transparency, data privacy breaches, cross-border data risks, cybersecurity attacks, child data misuse, weak accountability mechanisms, vendor lock-in and poor procurement governance.

The policy approach proposed by the group is rights-based and citizen-centred. It emphasises transparency, accountability, fairness, human oversight, data protection and accessible remedy mechanisms. These principles are essential where AI-enabled systems may affect access to public services or other high-impact decisions.

Recommended policy actions include national AI governance standards covering ethics, transparency, accountability, security and human rights protections; strengthened procurement governance through AI impact assessments, mandatory bias testing, vendor accountability provisions and data sovereignty protections; independent oversight mechanisms; human review for high-impact decisions; stronger data protection enforcement; and operational complaint, appeal and judicial recourse mechanisms.

AI holds significant potential for development in Africa, but deployment must be governed through privacy protection, data rights, transparency, accountability and reliable redress channels. These safeguards will help scale AI development while protecting citizens and strengthening trust in public institutions.

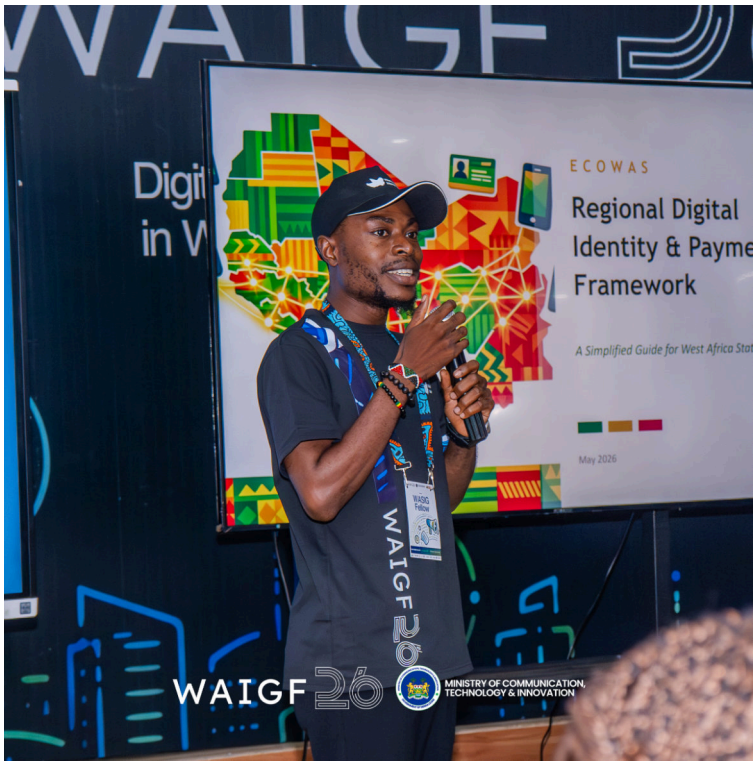
Annex C3. Group 3 Policy Brief. Digital Single Market and Interoperable Public Infrastructure

The group proposed a corridor for interoperable payments and digital identity involving Guinea, Sierra Leone and Senegal. Stakeholders agreed on a common vision: to build a secure, inclusive, open and standards-based regional infrastructure to facilitate trade, mobility and access to public services. They recognised that interoperability is not only technical, but also a matter of governance, trust and public interest.

The proposed roadmap includes political alignment and institutional framing over 0 to 6 months, common architecture and minimum harmonisation over 6 to 24 months, pilot corridor deployment over 24 to 60 months, regulated extension and market opening over 60 to 72 months, and regional institutionalisation and scaling over 72 to 120 months.

The group proposed harmonising regional layers that condition mutual trust and exchange, including identity trust frameworks, technical standards and APIs, minimum data schemas, cybersecurity rules, directories and routing, certification and compliance, minimum consumer protection, procurement and cloud portability rules, and common reporting. Differentiated national layers would include civil registry systems, enrolment modalities, user experience, languages and internal institutional organisation.

The governing principle is to harmonise what enables mutual trust and cross-border exchange while differentiating what belongs to sovereign implementation and local context. This principle offers a useful template for ECOWAS digital single market policy design.



Layer to harmonise	Value and reporting note
Identity trust framework	Mutual recognition, assurance levels and cross-border validation
Technical standards and APIs	Real interoperability among wallets, registries and payment service providers
Minimum data schema	Identity attributes, consent, logs and payment messages
Cybersecurity rules	Coherent incident response and minimum shared requirements
Directory, proxy and routing	Interoperable addressing for payments and verifications
Certification and compliance	Orderly market entry and quality control
Consumer protection	Transparency, refunds, remedies and complaint handling
Procurement and cloud portability	Avoidance of technical or commercial lock-in
Common reporting	Regional supervision and continuous improvement

Annex C4. Group 4 Policy Brief. Strengthening ECOWAS Cyber Resilience

Group 4 proposed a 72-hour regional response framework for ECOWAS cyber resilience. The problem statement recognises that West Africa's digital economy increasingly relies on digitised platforms, interconnected payment systems, customs platforms, national ID systems and government communication networks. A tabletop exercise highlighted gaps in regulatory and legal coordination, information sharing and regional crisis communication.

The group's participatory and regional approach emphasised that cyber resilience depends on governance, communication, legal cooperation and institutional trust, not only technology. Regional coordination is essential for protecting critical digital infrastructure and maintaining public trust across ECOWAS.

Core policy reforms include establishing an ECOWAS Cyber Response Centre, adopting a binding regional cyber incident protocol and harmonising legal frameworks for digital evidence and lawful access. Recommended actions for Member States include strengthening national CERTs and SOCs, ensuring 24/7 response capacity, aligning cybercrime and digital evidence laws, linking national crisis communication systems and training more people in cybersecurity skills.

The proposed implementation roadmap includes launching regional cyber coordination mechanisms, harmonising legal frameworks, conducting annual cyber drills and strengthening national CERT capacity. Risk mitigation should protect sovereignty through controlled intelligence sharing, support emerging CERTs through partnerships and ensure cybersecurity measures align with privacy protections. A coordinated regional framework would improve crisis preparedness, protect regional economies and strengthen trust in digital systems.

Gallery


WAIGF 26
MINISTRY OF CO
Suggested next steps
Track one issue


The Vision
Digi
in V
Shared Payment Switch
Faster, easier cross-border payments between all 15 ECOWAS countries through a connected system.


WAIGF 26
MINISTRY OF COMMUNICATION, TECHNOLOGY & INNOVATION


WAIGF 26
MINISTRY OF COMMUNICATION, TECHNOLOGY & INNOVATION

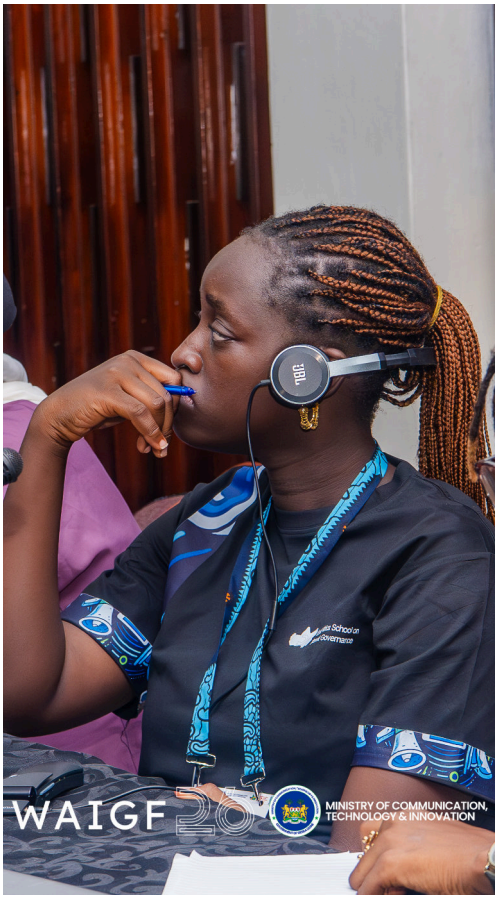

WAIGF 26
MINISTRY OF COMMUNICATION, TECHNOLOGY & INNOVATION


MINISTRY OF COMMUNICATION, TECHNOLOGY & INNOVATION
In Memoriam
Muriel Alapini


WAIGF 26
MINISTRY OF COMMUNICATION, TECHNOLOGY & INNOVATION


Coordinator
Coordinator


In Memoriam
Exercise 1: map the barriers
Small-group task • 15 minutes
WASIG Fellow
WAIGF 26
MINISTRY OF COMMUNICATION, TECHNOLOGY & INNOVATION


WAIGF 26
MINISTRY OF COMMUNICATION, TECHNOLOGY & INNOVATION