

PROJECT BRIDGE

National Digital Economy University-Led Research Clusters Programme



EXPRESSION OF INTEREST

submitted in response to

Reference No: NG-FMCIDE-544880-CS-QCBS

Project Number: P508383

RESEARCH CLUSTER
CLUSTER E

**Trust, Safety, Consumer Protection,
and Online Harms**

Visit the Expression of Interest website:

www.bridge-cluster-e.org.ng

Lead Institution: Bayero University, Kano

Submitted to: Federal Ministry of Communications, Innovation
and Digital Economy (FMCIDE)

Submission Date: April 2026

Contact: shmuhammad.csc@buk.edu.ng

1 Introduction and Submission Overview

Bayero University, Kano (BUK), submits this Expression of Interest, on behalf of a six-institution consortium, in response to the Terms of Reference for **Cluster E: Trust, Safety, Consumer Protection, and Online Harms**. The consortium combines three complementary strengths. First, it brings together a multidisciplinary university research base of four Nigerian and two United Kingdom institutions. Second, it incorporates operational digital platforms already deployed within Nigerian markets, including VigilSentinel for integrated cybersecurity operations, Wazobia Invoice for offline-first financial management in low-connectivity contexts, and SPIDVerify for identity verification and Know-Your-Customer compliance, each serving as both an applied case study and empirical research environment. Third, the consortium draws upon substantive policy and governance experience at executive and institutional levels, including a former vice-chancellor of applied sciences at Bayero University and a former commissioner for science and technology in Kano State.

Project BRIDGE will extend fibre-optic connectivity across at least 90,000 km of Nigerian territory, bringing millions of citizens into formal digital participation for the first time. Infrastructure deployment at this scale does not neutralise existing harms; it extends their reach to populations with limited prior exposure to online fraud, harmful content, and data exploitation. Protecting these populations requires regulatory frameworks and enforcement mechanisms grounded in evidence specific to Nigerian conditions: how abusive content propagates across Nigerian-language digital spaces, how deceptive practices operate within informal digital commerce, and how the Nigeria Data Protection Act 2023 performs in practice across the banking, health, and telecommunications sectors. That evidence base does not currently exist in sufficient form to support effective policy design or enforcement. This work is designed to produce it.

Our research is organised into six interconnected work packages (streams), each designed to produce both scientific outputs and actionable policy inputs: (i) online harms, hate speech, and content moderation; (ii) consumer protection in digital markets (fraud detection, phishing, informal digital economy harms); (iii) secure and privacy-preserving authentication for FinTech (behavioural biometrics, offline self-sovereign identity); (iv) trust, privacy, and data protection frameworks (NDPA 2023 enforcement, privacy-preserving health data); (v) youth online safety and digital literacy; and (vi) regulatory innovation and adaptive governance (comparative analysis with the EU DSA, UK Online Safety Act, and Kenya).

Each stream includes original mixed-methods research, fieldwork across Nigerian states, and a direct pathway to policy outputs, policy briefs, model regulations, technical frameworks, and open datasets, targeted at specific MDAs (NDPC, NITDA, CBN, FMCIDE, NCC, and the Federal Ministries of Health, Education, and Defence).

2 Consortium Structure and Participating Institutions

The consortium comprises six institutions: four Nigerian and two UK-based international partners. Bayero University, Kano serves as Lead Institution and contracting party, leading on digital trust, NLP, and online safety. Kano University of Science and Technology (Wudil), Federal University of Technology (Babura, Jigawa), and Northwest University (Kano) participate as joint-venture partners, contributing respectively AI and machine learning; recommender systems and data analytics; and deep learning, computer vision, and cybersecurity. York St John University and the University of Leicester participate as international sub-consultants, adding expertise in cybersecurity engineering and privacy-preserving identity management.

Table 1: Consortium composition and thematic responsibilities.

S/N	Institution	Country	Role	Thematic Focus
1	Bayero University, Kano	Nigeria	Lead Institution	Online Harms, NLP, AI Safety, Hate Speech Detection
2	Kano University of Science and Technology, Wudil	Nigeria	Nigerian Partner (AI Lead)	AI, Machine Learning, Data-Driven Systems
3	Federal University of Technology, Babura	Nigeria	Nigerian Partner	Recommender Systems, Data Analytics, cybersecurity, ICT
4	Northwest University, Kano	Nigeria	Nigerian Partner	Deep Learning, Feature Selection, Computer Vision, cybersecurity
5	York St John University	United Kingdom	International Partner	cybersecurity, Trust Systems, Data Privacy, IoT Security
6	University of Leicester	United Kingdom	International Partner	Cyber Security, Privacy, SSI, Fraud Prevention

3 Thematic Alignment and Relevance to Cluster E

The research expertise of the proposed consortium and existing platforms align directly with the priorities outlined in the Cluster E Terms of Reference. Our work spans online harms, content moderation, trust, cybersecurity, data privacy, and the governance and policy dimensions of these issues in the Nigerian context.

3.1 Online Harms, Hate Speech, and Content Moderation

Our consortium has built an unparalleled track record of research on online harms and hate speech in African languages.

- **AfriHate:** The first large-scale hate speech dataset spanning 15 African languages (including Hausa, Yoruba, Igbo and Nigerian-Pidgin), with native speaker annotations capturing socio-cultural context. AfriHate fills a critical gap in content moderation for Nigerian languages [1].
- **HERDPhobia:** The first dataset of Fulani ethnic hate speech in Nigerian social media (6,174 tweets in English, Hausa, and Nigerian-Pidgin), enabling detection of ethnicity-targeted abuse [2].
- **AfriSenti and NaijaSenti:** Sentiment analysis benchmarks for 14 African (110,000 tweets) and 4 Nigerian languages (Hausa, Igbo, Yorùbá, Nigerian Pidgin), used worldwide to study online polarisation and harms [5, 4].
- **POLAR:** Fine-grained benchmark for online polarization across 22 languages, supporting detection of harmful rhetorical tactics (stereotyping, vilification, dehumanization, extreme language, lack of empathy, invalidation) [6].

These resources are directly aligned with Cluster E’s research priorities on content moderation, platform accountability, online fraud, misinformation, and digital financial harms. By enabling accurate detection of harmful content within Nigeria’s diverse linguistic and cultural contexts, and by identifying polarising, deceptive, and abusive content patterns at scale, our existing research portfolio on online harms, hate speech, and content moderation provides a strong foundation for advanced, evidence-based, policy-driven outcomes.

3.2 Trust, Cybersecurity, and Data Privacy

Our consortium’s expertise in trust, cybersecurity, and data privacy includes:

- **FinTech Security:** WazoBia Invoice (www.wazobia-invoice.ng) is an offline-first, privacy-preserving fintech platforms developed through Dr. Usman’s research. It is built on zero-trust architecture and privacy-by-design principles, leveraging client-side (local-first) processing and self-sovereign data models, as well as encrypted, offline-first financial management systems that ensure security, resilience, and full user control over data.
- **Integrated FinTech Cybersecurity:** VigilSentinel (www.vigilsentinel.com), an integrated vulnerability management and financial cyber operations platform based on Dr. Usman’s research.
- **Trust-based Security:** Doctoral work on dynamic attribute trust models for secure wireless routing [7, 8]; best paper on voice biometric IoT authentication [9]; and privacy-by-design frameworks for healthcare IoT [10].
- **Self-Sovereign Identity and KYC:** SPIDVerify (spidverify.com), a SaaS platform for decentralised identity, KYC/AML, and GDPR-compliant reputation built on Dr. Shehu’s research [15].

- **Deep Learning for Cybersecurity:** Novel architectures for phishing detection (focal loss CNNs) and network intrusion detection (SWIN-VGG19) applied to consumer protection [26, 31].

These works directly support Cluster E priorities in consumer protection within digital markets and online financial ecosystems, data protection, privacy frameworks, and institutional enforcement, as well as online fraud and misinformation. Operational systems such as VigilSentinel, WazoBia Invoice, and SPIDVerify serve as practical case studies and real-world intervention testbeds for scalable trust, safety, and privacy-preserving technologies. Our prior experience and background in building and deploying these platforms will provide a strong foundation for delivering impactful, context-aware solutions. This established technical and research expertise will be leveraged to accelerate implementation, strengthen applied research outcomes, and ensure that outputs are both operationally viable and policy-relevant within Nigeria's digital trust and safety ecosystem.

3.3 Governance, Regulation, and Policy

Our team brings direct, hands-on governance and policy experience at executive, institutional, and national levels – including a former Vice Chancellor, a former Commissioner for Science and Technology, a director of a national ICT centre, and a dean with extensive curriculum and research governance responsibilities. These members have shaped government policy, institutional strategy, and infrastructure development in Nigerian contexts. Their expertise is critical to Cluster E's focus on governance models, adaptive regulatory approaches, and translating research insights into policy and economic development. Detailed profiles are provided in Sections 4.7 (Policy and Governance) and 4.8 (Professorial Lead).

This expertise is important to Cluster E's focus on "governance models", "adaptive regulatory approaches", and translating research insights into policy and economic development. Team members have direct experience shaping government policy, institutional strategy, and infrastructure development in Nigerian contexts.

3.4 Existing Platforms and Research Infrastructure

The consortium already operates platforms and projects that give Cluster E a running start.

3.4.1 VigilSentinel: Cybersecurity Operations Platform

VigilSentinel (www.vigilsentinel.com), founded by Dr. Usman, consolidates vulnerability assessment, endpoint monitoring, threat detection, log collection, and reporting in a single web application. Over 15 assessment types. Self-hosted or cloud-hosted.

Role-based access control. For this programme, it serves as a real-world testbed for evaluating digital safety interventions under Research Stream 3.

3.4.2 Wazobia Invoice: Secure FinTech for Underserved Markets

Wazobia Invoice (www.wazobia-invoice.ng), and Wazobia-books.ng (www.wazobia-books.ng) also Dr. Usman’s creation, help Nigerian businesses manage their financial records securely, even offline, and stay compliant. WazoBia-Invoice’s privacy-preserving, offline-first architecture makes it a working tool for financial inclusion in low-connectivity areas. For Research Streams 2 and 3, it offers a case study in consumer protection and trust in digital financial systems.

3.4.3 SPIDVerify: Identity Verification and KYC Compliance

SPIDVerify (spidverify.com), founded by Dr. Shehu, provides SaaS-based identity verification, KYC compliance, business onboarding, and AML screening, now serving 500+ organisations globally. It connects Dr. Shehu’s academic work on self-sovereign identity to a live commercial product. For Research Streams 2 and 4, SPIDVerify serves as both a case study in identity-based consumer protection and a testbed for evaluating how KYC and AML tools can be adapted to Nigerian regulatory and market conditions.

3.4.4 AfriSafe: Online Safety in the Age of AI

AfriSafe (<https://afrisafe.vercel.app>) founded by Dr. Shamsuddeen, addresses online safety challenges in the era of generative AI. The project builds resources, tools, and frameworks for understanding AI-related harms, deepfakes, AI-generated misinformation, automated hate speech. With programme funding, AfriSafe will sharpen its focus on Nigerian content moderation and develop safety resources built for Nigeria’s digital landscape. Research Streams 1 and 5 gain immediate infrastructure from day one.

These four operational platforms give the consortium research tools that most teams would spend their first year building. VigilSentinel, Wazobia Invoice, SPIDVerify, and AfriSafe, all built by consortium members, are already deployed in real environments. That reflects a team that treats the gap between academic insight and practical application.

4 Key Personnel (Indicative)

Table 2: Indicative key personnel for the Research Cluster.

S/N	Position	Name	Affiliation	Qualificatio	Experience
1	Consortium Lead	Dr. Shamsuddeen Hassan Muhammad	Bayero University, Kano	PhD Computer Science	15+ yrs; NLP, AI, online harms
2	Professorial Lead	Prof. Muhammad Yahuza Bello	Bayero University, Kano	PhD Mathematics	40+ yrs; academic leadership, IT, cryptography
3	Senior Research Specialist	Dr. Aminu Bello Usman	York St John University, UK	PhD Cyber Security	15+ yrs; cybersecurity, trust, privacy, fintech
4	Senior Research Specialist (NLP & Ethical AI)	Dr. Ibrahim Said Ahmad	Bayero University, Kano	PhD Computer Science	10+ yrs; NLP, ethical AI, emotion detection, LLMs
5	Senior Research Specialist (Data & Recommender Systems)	Assoc. Prof. Khalid Haruna	FUT Babura	PhD Computer Science	10+ yrs; recommender systems, data analytics, cybersecurity
6	Senior Research Specialist (Deep Learning & CV)	Dr. Abdulrauf Garba Sharifai	Northwest Univ., Kano	PhD Computer Science	11+ yrs; deep learning, feature selection, computer vision, cybersecurity
7	Senior Research Specialist (Cyber Security)	Dr. Abubakar-Sadiq Shehu	Univ. of Leicester / Bayero University, Kano	PhD Computer Science	12+ yrs; SSI, fraud prevention, GDPR, forensics
8	Senior Research Specialist (AI Lead)	Prof. Salisu Mamman Abdulrahman	ADUST Wudil	PhD Computer Science	15+ yrs; AI, ML, data-driven systems
9	Senior Research Specialist (Policy & Governance)	Prof. Bashir Shehu Galadanci	Bayero University, Kano	PhD Computer Engineering	30+ yrs; ICT policy, governance, software engineering

Continued on next page

Table 2 – continued from previous page

S/N	Position	Name	Affiliation	Qualificatio	Experience
10	Data & Analytics Team Lead	Dr. Hadiza Ali Umar	Bayero University, Kano	PhD Computer Science	10+ yrs; data analytics, AI policy, academic administration
11	Data & Analytics Specialist	Dr. Jaafar Zubairu Maitama	Bayero University, Kano	PhD Computer Science	8+ yrs; NLP, predictive modelling, large-scale data curation
12	Programme Administrator	Dr. Saminu Aliyu Kiri	Bayero University, Kano	PhD	Research administration and programme coordination

4.1 Consortium Lead: Dr. Shamsuddeen Hassan Muhammad

Dr. Muhammad holds a PhD in Computer Science from the University of Porto and an MSc from the University of Manchester, UK. He is Advanced Research Fellow and Google DeepMind Academic Fellow at Imperial College London, and Senior Lecturer at Bayero University, Kano. **Research impact: H-index 23 and over 4,900 Google Scholar citations.**

Selected achievements:

- **Grants:** PI/Co-PI on approximately **USD 5M** in competitive funding, including:
 - Co-PI, **Wellcome Trust (up to £3,000,000, 2025):** Generative AI for Anxiety, Depression and Psychosis.
 - Co-PI, **OpenAI (USD 50,000, 2025):** Cross-Cultural and Multilingual Mental Health Safety.
 - PI, **Open Data Collection Playbook and Collection Platform (USD 430,000, 2025).**
 - PI, **Lacuna Fund 2021 Language Datasets Award (USD 147,000, 2021):** Hate Speech Dataset for African Languages.
 - Co-PI, **Lacuna Fund (USD 120,000, 2022):** Nigerian Speech Corpus.
 - PI, **Lacuna Fund 2020 Language Datasets Award (USD 60,000, 2021):** Sentiment Analysis Dataset for African Languages.
 - PI, **Oracle Cloud Infrastructure Award (USD 50,000, 2022).**
 - PI, **Artificial Intelligence for Education Innovation Research Network in Africa (USD 40,000, 2022).**
 - Co-PI, **Google Research exploreCSR Award (USD 18,000, 2023).**
 - Co-PI, **Google Research TensorFlow Award (USD 10,000, 2023).**

- PI, **Nigerian AI Research Grant (₦5,000,000, 2023)**: Automatic Offensive Language Detection for Nigerian Languages.
- PI, **Lacuna Fund SemEval Shared Task Support (USD 8,500, 2021)**.
- **Datasets and benchmarks:** PI of AfriHate (NAACL 2025), hate speech dataset for 15 African languages; PI of BRIGHTER, emotion recognition dataset for 28 languages (ACL 2025 Best Resource Paper); co-developer of AfriSenti, NaijaSenti, HERDPhobia, and IrokoBench.
- **Awards:** ACL 2025 Best Resource Paper; SemEval 2025 Best Task Paper; NAACL 2025 Outstanding Paper; Deep Learning Indaba 2025 Best Paper; NeurIPS 2024 (C3NLP) Best Paper; AfricaNLP 2023 Best Paper; IJCNLP–AAACL 2023 Area Chair Award; EMNLP 2020 Wikimedia Research Award.
- **Supervision:** Three active PhD students. Visiting Lecturer at AIMS South Africa and AIMS Cameroon.
- Co-founder of HausaNLP and Arewa Data Science Academy.

4.2 Professorial Lead: Prof. Muhammad Yahuza Bello

Prof. Yahuza Bello served as the 10th Vice Chancellor of Bayero University, Kano (2015–2020). He holds a PhD in Mathematics from the University of Arkansas and has 40+ years of academic leadership experience.

What he brings to Cluster E:

- Founded Computer Science studies at BUK in 1990, which grew into a Faculty with over 1,500 graduates.
- Research in algebra and cryptography connects to the mathematical bedrock of cybersecurity and data protection.
- Served as Head of Mathematical Sciences, Dean of Science, Director of IT, Dean of Postgraduate Studies, and Deputy VC (Academics) before the vice-chancellorship.
- Supervised 6 PhD candidates, 37 MSc candidates, and over 50 BSc projects.
- Currently Pro-Chancellor of Al-Muhibbah Open University, Abuja.

4.3 Senior Research Specialist (Policy and Governance): Prof. Bashir Shehu Galadanci

Prof. Galadanci holds a BSc (First Class) from King Abdulaziz University and an MSc and PhD in computer engineering from Boston University, USA. He is a professor of software engineering at BUK with 30+ years of academic, policy, and governance experience.

What he brings to Cluster E:

- Served as special advisor to the governor of Kano State on ICT and education, then as commissioner for science and technology.
- Currently National Coordinator of the UBEC Digital Resource Centre, running digital education initiatives at a national scale.
- Held senior BUK positions: Dean of the Faculty of Computer Sciences and IT, Head of Software Engineering, Senate member, and council member.

4.4 Senior Research Specialist: Dr. Aminu Bello Usman

Dr. Usman is Associate Professor of Computer Science and Director of the Cybersecurity Research Group at York St John University. He previously served as Head of the School of Computer Science at the University of Sunderland and Head of the Department of Computer and Data Science at York St John University. He earned his PhD in Cyber Security from Auckland University of Technology and holds Senior Fellow (D3) status with Advance HE.

What he brings to Cluster E:

- Principal Investigator of *Cyber360: An Integrated Experiential Platform for Cyber Hygiene, Network Defence, and Embedded Systems Security Education*. The project produced open-source materials on [Embedded System Security](#), [Cyber Hygiene](#), and [Network Security](#).
- Recipient of ISIC 2025 Best Paper Award.
- Supervised and successfully graduated doctoral candidates in trust-based and voice biometric authentication, privacy-by-design frameworks for biometric verification, and secure authentication for financial applications, research areas at the heart of Cluster E.
- Patent pending: Zero-Trust Offline Point-of-Sale Network Using Single Permanent QR Code, Manager-Gated One-Time Codes, Dual-Key Encryption, and 12-Word Recovery Phrase. The research produced Wazobia Invoice.
- Founder of WazoBia Smartech Technologies, comprising: [WazoBia Invoice](#) (secure offline fintech for small enterprises), [WazoBia Books](#) (accounting software for Nigerian businesses), and [VigilSentinel](#) (integrated cybersecurity operations platform).
- His podcast series on deepfakes, which has reached many viewers across the UK and around the world, significantly raising awareness on generative AI and the rise of fake news in the era of artificial intelligence. The work was featured in the [UCAS Subject Spotlight](#), "Is Generative AI the Problem or the Solution?" Dr Aminu Usman explores the dual nature of generative AI, highlighting both its transformative potential for innovation and the risks associated with creating highly realistic deepfakes. Through this widely viewed session, he challenges policymakers to

engage critically with the ethical implications of AI and to consider its real-world applications in cybersecurity, directly aligning with the priorities of Cluster E.

4.5 Senior Research Specialist (Recommender Systems): Dr. Khalid Haruna

Associate Professor Khalid Haruna is Director of the Centre for Information Technology (CIT) and Head of Computer Science at the Federal University of Technology, Babura (FUT Babura), Jigawa State. He holds a PhD in Computer Science from the University of Malaya, Malaysia, an MSc (CGPA 5.00/5.00) from Bayero University Kano, and a First-Class BSc from BUK, where he was the best graduating student in Computer Science in both 2007, 2009, and 2011. He is ranked among the top 60 most-cited researchers worldwide on recommender systems according to Google Scholar, with over 50 publications in Q1 journals including IEEE Access, PLOS One, Scientometrics, and Computers and Security.

What he brings to Cluster E:

- Recognised as a top-60 global researcher on recommender systems, algorithms with direct application to personalised safety tools, fraud detection, and misinformation filtering in digital platforms.
- Has published extensively on cybersecurity, mobile touch-screen authentication, malware detection, and digital trust in peer-reviewed IEEE and Scopus-indexed journals, including a systematic literature review on mobile authentication security (Computers and Security, Q1).
- Won multiple research grants: two TETFund IBR grants as Lead Researcher (totalling over ₦4.2 million), a Malaysian Government FRGS grant (MYR 120,000), and University of Malaya Research Grants, demonstrating a strong record of securing competitive funding.
- Brought Bronze Award at the International Invention and Innovative Competition (2017), Best Paper Presenter at PgRES 2017 (University of Malaya), and 1st Runner-Up in the University of Malaya 3-Minute Thesis Competition (2018).

4.6 Senior Research Specialist (Deep Learning and Computer Vision): Dr. Abdulrauf Garba Sharifai

Dr. Sharifai is a Senior Lecturer in the Department of Computer Science, Faculty of Computing, Northwest University, Kano, with 11 years of teaching and research experience. He holds a PhD in Computer Science from University Science Malaysia, an M.Eng from Liaoning University of Technology (China), and a BSc from Bayero University, Kano. He specialises in deep learning.

What he brings to Cluster E:

- Research on hybrid deep learning for network intrusion detection (CyberComp 2024, IEEE) and phishing detection using focal loss and self-attention CNNs, addressing online fraud and cybercrime.
- Supervises two PhD candidates (semi-supervised object detection; multi-modal data retrieval) and four MSc candidates in deep learning and image processing.

4.7 Senior Research Specialist (Cyber Security): Dr. Abubakar-Sadiq Shehu

Dr. Shehu is a Teaching Fellow in Cyber Security at the University of Leicester and a Lecturer in Information Technology at Bayero University, Kano, where he was a pioneer staff member in cybersecurity within the Faculty of Computer Science. He also serves as a visiting Research Fellow at DECaDE: the Centre for the Decentralised Digital Economy, University of Surrey — one of the UK's Academic Centres of Excellence in Cyber Security Research (ACE-CSR), recognised as a gold standard for British research and learning in cybersecurity. He has supervised over 20 postgraduate students. He holds a PhD in Computer Science (Information Systems Security) from the University of Porto, Portugal, with a thesis titled "Establishing Secure and Privacy-Preserving Digital Identity with Self-Sovereign Identity." His doctoral research focused on giving individuals control over their own digital identities without relying on central authorities, enhancing both security and privacy. He also holds an MSc in Business Information Systems from the University of East London, United Kingdom, and a BSc in Computer Science (Digital Systems Security) from the University of Wollongong, Australia. His career spans over 12 years across academia, consultancy, big tech (Google, Apple), banking, and international research.

What he brings to Cluster E:

- Co-team researcher on NanoSTIMA (€2.5M EU Horizon 2020, INESC TEC Porto), building secure health data infrastructure used for Portugal's COVID vaccine tracking system.
- Research Fellow on DECaDE (£6M funded) at the Surrey Centre for Cyber Security. One of the few Gold centres for cybersecurity research and learning in the UK. The programme's work on a governance framework, particularly a secure digital economy in supply chains.
- Pioneer Search Language Engineer at Google (2022–2024): designed and optimised NLP algorithms and language models for Hausa and Yoruba, managing projects from pilot to production.
- Fraud Prevention Specialist at Apple (2020–2022): led fraud prevention across all payment channels, monitored debit card fraud alerts, identified fraud patterns by country and merchant, and reviewed VISA CAMS and FICO alerts.
- Technical officer at N26, largest mobile bank in Germany (2019–2020): Delivered

IT operational and technical support for hardware and software systems, ranging from peripheral devices to core infrastructure, that underpin customer transactions.

- Risk Officer at Unity Bank PLC (Nigeria, 2013–2015): conducted KYC/customer due diligence, developed cybersecurity strategies, and prepared risk reports for senior management, grounding his academic work in Nigerian banking realities.
- Founded SPIDVerify (spidverify.com): SaaS platform for identity verification, KYC compliance, business onboarding, and AML screening. Spidverify also serves data protection consultancy.
- Holds certifications in CCNA, Security+, CEH, GDPR Compliance, and ISO Security Standards.

4.8 Senior Research Specialist (AI Lead): Prof. Salisu Mamman Abdulrahman

Professor Abdulrahman is a Professor of Artificial Intelligence (Machine Learning) and dean of the Faculty of Computing and Mathematical Sciences at Aliko Dangote University of Science and Technology (ADUST), Wudil. He holds a PhD from the MAPi Joint Doctoral Programme in Computer Science (Universities of Minho, Aveiro, and Porto, Portugal, the same programme as the consortium lead), an MSc from Bayero University Kano, and a first-class BSc from ADUST Wudil. His Google Scholar profile records over 300 citations across machine learning, algorithm selection, and data-driven research.

What he brings to Cluster E:

- As Dean of the Faculty of Computing and Mathematical Sciences at ADUST Wudil, he provides institutional leadership and governance capacity, supporting coordination between the two Kano-based Nigerian partner institutions in Nigeria.
- Research expertise in machine learning, algorithm selection, and meta-learning, published in *Machine Learning* (Springer, 2018) and the IEEE NIGERCON 2024 proceedings, provides the analytical foundations for automated detection of online harms, fraud, and deceptive practices.
- Extensive supervisory track record at MSc and PhD levels in AI and machine learning, strengthening the consortium's doctoral cohort.

4.9 Senior Research Specialist (NLP and Ethical AI): Dr. Ibrahim Said Ahmad

Dr Ibrahim Said Ahmad is a senior lecturer in the Department of Information Technology at Bayero University, Kano, with over 10 years of research and teaching experience across NLP, ethical AI, and multilingual machine learning. He holds a PhD from Universiti Kebangsaan Malaysia and an MSc from the University of Nottingham, Malaysia.

His research record spans 40+ peer-reviewed publications, 10+ as first author, across NLP, emotion detection, sentiment analysis, and responsible AI.

What he brings to Cluster E:

- Co-author and active contributor to AfriHate, the first labelled hate speech dataset for 15 African languages, and to NaijaSenti, the first large-scale multilingual sentiment corpus for Nigerian languages (Hausa, Igbo, Nigerian Pidgin, and Yorùbá).
- Supervised MSc researchers in fake news detection, vulnerability exploitation prediction, and negative purchase intent classification, research themes with direct applications to online harm detection and consumer protection.
- Won over USD 300,000 in competitive grants as PI and Co-PI, including two Google Research exploreCSR awards, two TensorFlow awards, Lacuna Fund grants totalling USD 168,000+, an Oracle OCI Award, and a Google COVID-19 Research Grant.

4.10 Data and Analytics Team: Dr. Hadiza Ali Umar

The consortium's Data and Analytics team comprises four experienced researchers from BUK. Dr. Hadiza Ali Umar leads the team, drawing on her roles as Head of Department and Secretary of the AI Policy Development Committee to coordinate data activities, reporting, and stakeholder communication. **Dr. Jaafar Zubairu Maitama** serves as Data and Analytics Specialist, bringing proven expertise in NLP and predictive modeling to analyse online harms, fraud patterns, and digital trust in Nigerian contexts. **Maryam Ibrahim Mukhtar** contributes software engineering and LLM-related research, along with administrative experience as an examination and admission officer, to support data workflows. **Sanah Abdullah Muaz** adds deep learning and sentiment analysis skills, supported by her international conference presentations. Together, the team combines high-impact research, analytics, and academic administration to coordinate all data activities throughout the programme.

4.11 Programme Administrator: Dr. Saminu Aliyu Kiri

Dr. Kiri, based at BUK, will coordinate research activities across all six institutions: managing documentation, tracking deliverables, supporting collaboration between Nigerian and international partners, and ensuring outputs are submitted on time. His familiarity with BUK's research systems and the consortium's institutional landscape positions him well for programme coordination, financial reporting, and stakeholder communication across the 36-month assignment.

5 Institutional Experience and Capacity

5.1 Nigerian Partner Institutions

5.1.1 Bayero University, Kano (Lead Institution)

BUK is one of Nigeria’s leading federal universities. Its Department of Computer Science and Faculty of Computer Science and Information Technology punch above their weight in NLP, AI, and digital safety research. BUK has managed grants from the Lacuna Fund, Google Research, and Oracle, and its research governance structures support multi-institutional collaboration. BUK is the institutional home of HausaNLP and Arewa Data Science, two of the most active NLP research communities.

5.1.2 Kano University of Science and Technology, Wudil

ADUST Wudil, a state university in Kano, houses a Faculty of Computing and Mathematical Sciences with growing research output in AI, machine learning, and data science. Under the deanship of Prof. Abdulrahman, the faculty has developed strong doctoral and MSc programmes in AI and machine learning. ADUST Wudil and BUK together form a natural Kano-based research corridor, sharing research networks, mentoring capacity, and access to state-level digital economy stakeholders.

5.1.3 Federal University of Technology, Babura, Jigawa State

The Federal University of Technology, Babura (FUT Babura) is a federal university in Jigawa State, northern Nigeria. Its Centre for Information Technology (CIT), directed by Assoc. Prof. Haruna, provides internet services, ICT infrastructure management, software development, and ICT consultancy for the university community. FUT Babura extends the consortium’s geographic footprint from Kano into Jigawa State, widening its reach into underserved northern communities directly relevant to the Programme’s digital inclusion mandate.

5.1.4 Northwest University, Kano

Northwest University, Kano is a Nigerian state university with a Faculty of Computing. Through Dr. Sharifai, the consortium gains expertise in deep learning, computer vision, feature selection, and cybersecurity. His research on network intrusion detection, phishing detection, and image-based anomaly detection, all published at IEEE venues, adds a complementary technical layer to the consortium’s digital safety and consumer protection work. His BSc from BUK and 11 years of continuous teaching experience in northern Nigeria ensure effective coordination with the Lead Institution and access to the same regional research networks.

5.2 International Partner Institutions

5.2.1 York St John University, UK

York St John hosts the cybersecurity Research Group directed by Dr. Usman. Active programmes in trust-based systems, data privacy, biometric security, IoT, and the Cyber360 education platform add UK cybersecurity network access and international research standards. The group's doctoral supervision record in biometric authentication and privacy-by-design frameworks directly adds to the consortium's research capacity.

5.2.2 University of Leicester, UK

The University of Leicester's School of Computing and Mathematical Sciences runs active programmes in cybersecurity, information security, and digital forensics. Through Dr. Shehu, who also holds a lectureship at BUK, Leicester contributes expertise in self-sovereign identity, GDPR-compliant privacy systems, fraud prevention, and forensic investigation. His prior appointments at the Surrey Centre for Cyber Security (DECaDE, £6M) and INESC TEC Porto (NanoSTIMA, €2.5M EU Horizon 2020) give the consortium access to established European cybersecurity research networks. His dual Nigerian-UK appointment bridges international research standards and Nigerian institutional needs directly.

6 Doctoral and Post-Doctoral Research Capacity

One of this Programme's most valuable long-term outcomes won't be a report or a dataset. It will be people. A cohort of researchers who can sustain top-tier work in digital trust and safety long after the funding ends. We've already built the infrastructure to prove it.

6.1 A Proven Mentoring Track Record

The Consortium Lead, Dr. Muhammad, co-founded two community-driven initiatives that have trained hundreds of Nigerian students and early-career researchers:

- **Arewa Data Science Academy** (arewadatascience.github.io) is a free, 16-week fellowship in data science, machine learning, and deep learning. Backed by Google Research, TensorFlow, and BUK, the Academy has graduated multiple cohorts, three in machine learning, two in deep learning, with a deliberate focus on under-represented groups including women.
- **HausaNLP** (hausanlp.github.io) is an open-source community for Hausa NLP, co-founded by Dr. Muhammad. The community has produced work used by researchers worldwide. Its curated catalogue (catalog.hausanlp.org) aggregates all known Hausa NLP resources.

This is the mentoring infrastructure that this programme will draw upon. Fellows and mentors from these communities represent a ready pool of junior and mid-career researchers who can contribute to Cluster E as researchers and PhD candidate.

6.2 Meeting the Programme’s Researcher Requirements

We commit to recruiting at least fifteen postdoctoral researchers and fifteen PhD candidates. The objective is to develop researchers who can integrate technical expertise with policy engagement, producing evidence and translating it effectively for decision-makers. The indicative allocation is summarised below; final assignments will be confirmed in the Inception Report.

Table 3: Indicative allocation of post-doctoral researchers and doctoral candidates across the consortium, with primary research streams identified for each institution.

S/N	Institution	Post-Docs	PhD Candidates	Primary Streams
1	Bayero University, Kano (Lead)	5	5	1, 2, 4, 6
2	Kano University of Science and Technology, Wudil	3	3	2, 3
3	Federal University of Technology, Babura	2	2	3, 5
4	Northwest University, Kano	2	2	5, 6
5	York St John University	2	2	1, 4
6	University of Leicester	1	1	4, 6
Total		15	15	—

- **Postdoctoral researchers:** Community networks (Masakhane, HausaNLP, Arewa Data Science, Black in AI) and institutional affiliations connect us to a broad postdoctoral talent pool. Several Arewa Data Science alumni and HausaNLP contributors have since completed or are completing doctoral degrees, creating a natural feeder into postdoctoral positions.
- **PhD candidates:** BUK, FUT Babura, ADUST Wudil, and our international partners run active doctoral programmes. We will recruit PhD candidates whose dissertations address nationally relevant Cluster E questions.
- **Professorial Lead:** Professor Yahuza Bello (former BUK Vice Chancellor) provides academic leadership and quality assurance. His governance experience and institutional networks give the programme the stature it needs.
- **Reach beyond the consortium:** Through HausaNLP, Arewa Data Science, AfriSafe, and Masakhane, the programme’s impact won’t stay locked inside six institutions. These open networks pull in emerging researchers across Nigeria and the continent.

When this programme ends in 36 months, the community infrastructure will still be running.

7 Indicative Research Programme

The consortium proposes six interconnected research streams that together form a coherent programme of work aligned with Cluster E’s objectives. Each stream is designed to produce both scientific outputs and actionable policy inputs. The programme is informed by the consortium’s existing platforms (VigilSentinel, Wazobia Invoice, SPIDVerify, and AfriSafe); completed funded research projects [Lacuna Fund Awardees 2021](#), [DECaDE project](#), [NANOSTIMA Project](#), and [NAIRS Research Grantee](#); and builds on state-of-the-art research in NLP, cybersecurity, and governance.



Figure 1: Cluster E Research Streams, Interdependencies, Outputs, and Impact Pathway

As shown in Figure 1, the streams are interdependent: Streams 1–3 generate core technical assets (detection models, fraud tools, authentication frameworks); Streams 4–6 provide governance, privacy, and regulatory integration.

7.1 Research Stream 1: Online Harms, Hate Speech, and Content Moderation

Objectives:

- Build multilingual hate speech and abusive language detection systems for Nigerian languages, initially capturing Hausa, Igbo, Pidgin and Yorùbá).
- Evaluate major platforms’ content moderation effectiveness in Nigerian contexts.
- Design community-informed governance models for content moderation.
- Investigate political polarisation, misinformation, and radicalisation in Nigerian digital spaces.

Key Research Questions:

Table 4: Research Stream 1: Online harms, hate speech, and content moderation – key research questions and intended policy outputs.

S/N	Lead Researcher(s)	Research Question	Policy Output
1	Dr. Muhammad, Dr. Ahmad, Prof. Galadanci	How does hate speech in Nigerian languages differ across election cycles, and what detection models achieve acceptable false-positive rates?	Detection model + brief for INEC/NITDA
2	Dr. Muhammad, Dr. Ahmad	To what extent do platforms' moderation systems fail Nigerian-language hate speech, and what appeals mechanisms are appropriate?	Policy brief for NCC/FMCIDE
3	Dr. Muhammad, Prof. Galadanci	What are the pathways from online radicalisation to offline violence in northern Nigeria?	Risk framework for ONSA/Defence

Methodology:

- **Data:** Extend AfriHate dataset (NAACL 2025) to five additional Nigerian languages; collect new labelled data from social media (Twitter, Facebook, WhatsApp) during election periods.
- **Analysis:** Fine-tune multilingual LLMs (AfriBERTa, ChatGPT, Gemini) with low-resource adaptation; compare platform moderation via systematic content submission and appeal tracking.
- **Fieldwork:** Focus groups with content moderators across six geopolitical zones.

Milestones and Deliverables:

- M6: Extended AfriHate dataset (v2.0) with five new languages.
- M12: Baseline hate speech detection models for six Nigerian languages.
- M24: Platform moderation audit report.
- M36: Final policy brief and radicalisation risk framework.

Policy Alignment: Electoral Act 2022 (hate speech provisions); NITDA Code of Practice (draft); Cybercrimes Act 2015.

7.2 Research Stream 2: Consumer Protection in Digital Markets

Objectives:

- Map online fraud, digital financial harms, and consumer exploitation in Nigeria.

- Develop NLP tools for detecting fraudulent content and phishing in Nigerian languages.
- Assess existing consumer protection mechanisms (FCCPC, CBN).
- Study how women, youth, and rural communities experience digital marketplaces.

Key Research Questions:

S/N	Lead Researcher(s)	Research Question	Policy Output
1	Dr. Haruna, Dr. Sharifai, Dr. Shehu	How do phishing and deceptive digital lending practices target low-literacy users?	Fraud detection prototype + CBN brief
2	Dr. Haruna, Dr. Sharifai	What are the most common consumer harms in informal digital economy (WhatsApp trade, social commerce)?	Consumer harm taxonomy for FCCPC
3	Dr. Usman, Dr. Shehu	How effective are e-commerce dispute resolution mechanisms for rural women traders?	Policy brief for FMCIDE/State govts

Table 5: Research Stream 2: Consumer protection in digital markets – key research questions and intended policy outputs.

Methodology:

- **Data:** Collect phishing and scam messages via crowd-sourcing (Nigerian Fraud Reporting System); scrape social commerce groups (WhatsApp, Facebook Marketplace).
- **Analysis:** NLP classification (phishing detection using focal loss + self-attention CNNs, building on Dr. Sharifai’s IEEE CyberComp 2024 work); survey of 2,000 digital consumers across three states.
- **Fieldwork:** Mystery shopping in informal digital markets; interviews with FCCPC and CBN consumer protection desks.

Milestones and Deliverables:

- M9: Nigerian Phishing Corpus (5,000+ labelled messages in Hausa, Pidgin, English).
- M18: Fraud detection API prototype.
- M27: Consumer harm taxonomy and regulatory gap analysis.
- M36: Final policy recommendations for CBN and FCCPC.

Policy Alignment: CBN Circular on Digital Financial Services (2023); BOFIA 2020; FCCPA 2018.

7.3 Research Stream 3: Secure and Privacy-Preserving Authentication for Trustworthy FinTech

Objectives:

- Design multi-modal continuous authentication frameworks for Nigerian FinTech.
- Address challenges of underserved groups (rural, informal workers, PWDs) by reducing reliance on static credentials.
- Produce policy guidance on balancing fraud prevention and data privacy.

Key Research Questions:

Table 6: Research Stream 3: Secure and privacy-preserving authentication for FinTech – key research questions and intended policy outputs.

S/N	Lead Researcher(s)	Research Question	Policy Output
1	Dr. Usman, Dr. Shehu, Prof. Bello	Can behavioural biometrics reduce fraud in agent banking while being usable for low-literacy agents?	Technical framework + CBN guidance
2	Dr. Shehu, Dr. Usman	What are barriers to SSI adoption for informal workers, and how can SPIDVerify adapt for offline-first use?	SSI prototype + brief for CBN/NDPC
3	Dr. Usman, Dr. Muhammad	How do rural users perceive security vs convenience in mobile money authentication?	User study + design recommendations

Methodology:

- **Data:** Behavioural biometric logs from Wazobia Invoice and SPIDVerify; new user study with 300 rural mobile money agents.
- **Analysis:** Continuous authentication using swipe patterns, typing rhythm, and device context; privacy-preserving aggregation using secure multi-party computation (inspired by completed EU-funded projects (NanoSTIMA WP1)).
- **Prototyping:** Extend Wazobia Invoice with a behavioural biometric module; test offline-first SSI on low-end Android devices.

Milestones and Deliverables:

- M12: Behavioural biometric authentication prototype.

- M24: Offline SSI module for SPIDVerify.
- M30: User study report and design recommendations.
- M36: Policy guidance note for CBN (authentication standards for agent banking).

Policy Alignment: CBN Agent Banking Guidelines (2021); NDPA 2023 (biometric data as sensitive); Nigeria Startup Act 2022.

7.4 Research Stream 4: Trust, Privacy, and Data Protection Frameworks

Objectives:

- Evaluate enforcement of NDPA 2023 across banking, health, and telecoms sectors.
- Develop privacy-preserving frameworks for digital identity, health systems, and FinTech.
- Investigate public trust in digital platforms and government services.
- Compare data protection enforcement models across African and international jurisdictions.

Key Research Questions:

Table 7: Research Stream 4: Trust, privacy, and data protection frameworks – key research questions and intended policy outputs.

S/N	Lead Researcher(s)	Research Question	Policy Output
1	Dr. Shehu, Dr. Usman, Dr. Muhammad	How consistently is NDPA 2023 enforced across sectors?	Enforcement audit + NDPC recommendations
2	Dr. Shehu, Dr. Usman	What privacy-preserving architecture enables secure health data sharing without violating NDPA?	White paper for Health Ministry/NDPC
3	Dr. Muhammad, Prof. Galadanci	How does public trust in government digital ID compare to private FinTech KYC?	Trust survey + brief for NIMC/NDPC

Methodology:

- **Legal analysis:** Systematic review of NDPA enforcement actions, court cases, and NDPC guidance.
- **Technical:** Prototype privacy-preserving health data repository using secure multi-party computation.

- **Survey:** National trust survey (n=3,000) stratified by region, age, gender, and digital literacy.

Milestones and Deliverables:

- M12: Comparative analysis of data protection enforcement (Nigeria vs Kenya, South Africa, EU).
- M24: Privacy-preserving health data sharing prototype.
- M30: National trust survey report.
- M36: Policy reform recommendations for NDPC.

Policy Alignment: NDPA 2023; National Digital Health Strategy (2021–2025); NDPC enforcement guidelines (draft).

7.5 Research Stream 5: Youth Online Safety and Digital Literacy**Objectives:**

- Assess cyberbullying, harmful content exposure, and online exploitation affecting Nigerian youth.
- Evaluate existing digital literacy programmes (UBEC, NITDA).
- Develop age-appropriate safety tools and resources in Nigerian languages.

Key Research Questions:

Table 8: Research Stream 5: Youth online safety and digital literacy – key research questions and intended policy outputs.

S/N	Lead Researcher(s)	Research Question	Policy Output
1	Dr. Ahmad, Dr. Haruna, Dr. Muhammad	What online harms are most prevalent among adolescents in urban vs rural schools?	Youth safety survey + curriculum module
2	Dr. Ahmad, Prof. Galadanci	Which digital literacy programmes actually reduce risky behaviour?	Evaluation brief for Education Ministry
3	Dr. Ahmad, Dr. Muhammad	How do gender norms affect girls' exposure and reporting of online harms?	Gender analysis + brief for Women Affairs

Methodology:

- **Survey:** 2,000 secondary school students across the federation, in predominantly rural communities (ages 13–18).

- **Focus groups:** 20 schools (10 rural, 10 urban) with separate groups for boys and girls.
- **Intervention:** Co-design and test age-appropriate safety messaging in Hausa, Pidgin, and English.

Milestones and Deliverables:

- M12: Baseline report on youth online harms.
- M24: Evaluation of existing digital literacy programmes.
- M30: Prototype safety toolkit (two Nigerian languages).
- M36: Curriculum recommendations for Federal Ministry of Education.

Policy Alignment: Child Rights Act 2003; UBEC Digital Resource Center (Prof. Galadanci as National Coordinator); National Gender Policy.

7.6 Research Stream 6: Regulatory Innovation and Adaptive Governance

Objectives:

- Compare digital trust and safety regulatory frameworks across EU, UK, Kenya, and India.
- Design adaptive governance mechanisms for Nigerian context.
- Assess institutional capacity of NDPC, NITDA, NCC, CBN to enforce digital safety standards.

Key Research Questions:

Table 9: Research Stream 6: Regulatory innovation and adaptive governance – key research questions and intended policy outputs.

S/N	Lead Researcher(s)	Research Question	Policy Output
1	Prof. Galadanci, Prof. Abdulrahman, Dr. Shehu	What can Nigeria learn from EU DSA, UK Online Safety Act, and Kenya's enforcement?	Comparative analysis + model framework for NITDA
2	Prof. Galadanci, Dr. Shehu	Do current institutional arrangements create regulatory gaps or overlaps?	Institutional mapping + recommendations for FMCIDE
3	Prof. Abdulrahman, Dr. Usman	How can innovation sandboxes include consumer protection safeguards?	Sandbox governance framework

Methodology:

- **Comparative legal analysis:** Review of legislation, regulations, and enforcement actions in five jurisdictions.
- **Institutional mapping:** Interviews with officials from NDPC, NITDA, NCC, CBN, and FMCIDE.
- **Case study:** Analyse three existing sandboxes (FinTech, healthtech, agritech) for consumer protection gaps.

Milestones and Deliverables:

- M12: Comparative regulatory report.
- M24: Institutional capacity assessment.
- M30: Adaptive governance framework.
- M36: Model legislation / regulatory code for NITDA and NDPC.

Policy Alignment: NITDA Code of Practice (draft); Nigeria Startup Act 2022; ECOWAS data protection directive.

7.7 Expected Scientific Outcomes and Exploitation

Each research stream is designed to produce both academic outputs and practical, policy-ready deliverables. The consortium commits to the following quantitative targets over the 36-month programme.

7.7.1 Scientific Publications and Datasets

- **Journal papers:** 12 submissions to Q1 peer-reviewed journals (e.g., *NAACL*, *ACL*, *IEEE S&P*, *Computers & Security*, *Telematics and Informatics*).
- **Conference papers:** 24 presentations at major venues (e.g., *NeurIPS*, *ICLR*, *ICWSM*, *IEEE CyberComp*, *AfricaNLP*).
- **Datasets:** 6 new publicly released corpora (extended *AfriHate*; Nigerian Phishing Corpus; Youth Online Safety Survey; FinTech Trust Dataset; Deepfake Benchmark; NDPA Enforcement Case Tracker). All datasets will be deposited in open repositories (Zenodo, Hugging Face) with DOIs, codebooks, and machine-readable formats.
- **Prototypes:** 4 functional software demonstrations (behavioural biometric authentication module for Wazobia Invoice; offline SSI extension for SPIDVerify; phishing detection API; privacy-preserving health data repository).

7.7.2 Policy and Institutional Outputs

- **Policy briefs:** 18 structured, actionable briefs (one per research stream per six months), tailored to specific MDAs and timed to align with policy windows (e.g., NDPC guideline drafting, CBN circular revisions, NITDA Code of Practice consultations).
- **Model frameworks:** 3 draft regulatory or technical frameworks (content moderation governance model; behavioural biometric authentication standard for agent banking; adaptive sandbox governance mechanism).
- **National trust survey:** One nationally representative survey on digital trust, data protection awareness, and online safety, with regional, gender, and age disaggregation.

7.7.3 Doctoral and Capacity Development

- **PhD candidates:** 15 PhD candidates fully supported and supervised, each producing a dissertation aligned with Cluster E themes.
- **Postdoctoral researchers:** 15 postdoctoral researchers completed, with at least 10 placed in Nigerian universities or research institutions (pathway to permanent academic appointments as outlined in Section 6.2).
- **Training:** Structured annual training in research ethics, NDPA 2023 compliance, policy communication, and grant writing for all early-career researchers.

7.7.4 Exploitation and Impact Pathways

Research outputs will be exploited through multiple channels:

- **Regulatory uptake:** Policy briefs and model frameworks will be formally submitted to NDPC, NITDA, CBN, FCCPC, and FMCIDE, with follow-up workshops to support adoption. We will track citations in official gazettes, guidelines, and circulars.
- **Industry adoption:** Technical prototypes (behavioural biometrics, offline SSI, phishing detection) will be integrated into existing consortium platforms (Wazobia Invoice, SPIDVerify, VigilSentinel), demonstrating real-world feasibility. We will seek at least one commercial deployment within a Nigerian FinTech (target: agent banking network).
- **Open science:** All datasets, codebooks, and analysis scripts will be released under CC-BY 4.0 licenses to enable replication and secondary research by the wider Nigerian and African research community.
- **Community dissemination:** Findings will be shared via HausaNLP, Arewa Data Science Academy, Masakhane, and AfriSafe channels, reaching practitioners, civil

society, and policymakers beyond formal academic circles.

- **Doctoral pipeline:** The programme will produce a cohort of PhD graduates with hands-on experience in policy-relevant digital trust research, creating a sustainable talent pool for Nigerian universities and government agencies.

7.7.5 Success Metrics and Monitoring

Progress against the above targets will be reported quarterly in the Technical and Financial Progress Reports (see Section 4 of ToR). A midterm review (Month 18) will assess publication pipelines, policy engagement effectiveness, and researcher retention, with corrective actions where needed.

7.8 Summary of Research Streams by Policy Sector

Table 10: Mapping of research streams to policy sectors, lead Ministries, Departments, and Agencies, principal outputs, and target completion milestones.

S/N	Stream	Sector	Lead MDA	Key Output	Timeline
1	Online Harms, Content Moderation	Defence / Elections	ONSA, INEC, NITDA	Hate speech detection + radicalisation risk framework	M36
2	Consumer Protection in Digital Markets	Consumer Finance	CBN, FCCPC	Fraud detection prototype + harm taxonomy	M36
3	Secure Authentication for FinTech	FinTech Innovation	CBN, NDPC	Behavioural biometrics + offline SSI	M30
4	Trust, Privacy & Data Protection	Data Protection	NDPC, Health Ministry	Enforcement audit + privacy-preserving health data	M36
5	Youth Online Safety & Digital Literacy	Youth	Education Ministry, UBEC	Safety toolkit + curriculum evaluation	M36
6	Regulatory Innovation & Adaptive Governance	Regulation	NITDA, FMCIDE	Comparative analysis + model framework	M36

8 Policy Outreach and Impact Pathways

Effective translation of research into policy requires structured engagement, clear accountability mechanisms, and demonstrable pathways to impact. This section details the consortium’s outreach strategy and the frameworks required by the Terms of Reference to ensure accountability, compliance, and measurable outcomes.

8.1 Target MDAs, Policy Instruments, and Inclusion of Unserved and Underserved Populations

The following Ministries, Departments, and Agencies (MDAs) are the primary recipients of our policy outputs:

- Federal Ministry of Communications, Innovation and Digital Economy (FMCIDE)
- Nigeria Data Protection Commission (NDPC)
- National Information Technology Development Agency (NITDA)
- Nigerian Communications Commission (NCC)
- Central Bank of Nigeria (CBN)
- Federal Competition and Consumer Protection Commission (FCCPC)
- Federal Ministry of Education
- Federal Ministry of Health
- Federal Ministry of Defence
- National Orientation Agency
- National Assembly (relevant committees)
- State governments

Policy instruments: Regular policy briefs (18 over 36 months), executive summaries, slide decks, and model regulatory frameworks, each timed to specific policy windows (e.g., NDPC guideline drafting Q4 2026, CBN circular revisions, NITDA Code consultations). All policy outputs will explicitly address the needs and vulnerabilities of **unserved and underserved populations**, including rural communities, women, youth, informal workers, persons with disabilities, and micro and small enterprises. Research findings will be disaggregated by these categories where feasible, and policy recommendations will include targeted actions for each group.

Stakeholder dialogue: Quarterly policy labs while liaising with state and local governments, co-chaired by FMCIDE and NDPC, with participation from tech platforms, fintechs, civil society, and representatives of unserved and underserved communities (e.g., rural women traders, youth groups, informal worker associations, and disability advocacy organisations).

Capacity building: Annual training workshops for government officials (NDPC enforcement staff, CBN consumer protection desk, NITDA platform regulation unit) on digital trust, online safety, and evidence-based policymaking, with a module on inclusive design for vulnerable populations.

Open data: All datasets delivered in reusable, machine-readable formats (CSV, JSON, Parquet) with DOIs, codebooks, and CC-BY 4.0 licenses. Datasets will include demo-

graphic variables to enable analysis of differential impacts on underserved groups.

8.2 Theory of Change

If Nigerian universities co-produce locally-grounded evidence on online harms, consumer protection, identity, privacy, and governance, and that evidence is delivered as policy briefs, model regulations, technical prototypes, and open datasets to specific MDAs at identified decision points, then Nigeria’s regulatory institutions will adopt better-calibrated rules and enforcement practices, leading to measurably safer digital experiences for unserved and underserved Nigerians as Project BRIDGE expands connectivity.

Causal chain: Inputs (consortium expertise, datasets, platforms) → Activities (mixed-methods research, fieldwork, prototyping) → Outputs (12 Q1 papers, 24 conference papers, 18 policy briefs, 6 datasets, 4 platform extensions) → Outcomes (regulatory adoption, institutional capacity, doctoral pipeline) → Impact (trustworthy digital economy, reduced consumer harm, retained citizen confidence in BRIDGE infrastructure).

8.3 Results Framework

Table 11: Results framework with 36-month targets across output, outcome, and impact levels.

S/N	Level	Indicator	Baseline	Target
1	Output	Policy briefs submitted	0	18
2	Output	Curated machine-readable datasets	3	6 new datasets
3	Outcome	Government citations or direct use of research	0	≥3 distinct citations
4	Outcome	Postdocs/PhDs placed in Nigerian academia	0	≥10
5	Impact	Adoption of privacy-preserving framework by a Nigerian FinTech	0	≥1

Quarterly progress reported; targets refined with QA Firm during Inception Phase.

8.4 Risk Framework

Table 12: Risk register with mitigation measures

S/N	Category	Specific Risk	Likelihood	Impact	Mitigation
1	Political-economy	Bureaucratic delays in MDA engagement for platform testing and data sharing	Medium	High	Early MoUs; embedded liaisons; quarterly policy labs
2	Operational	Logistics constraints (power, internet, device availability) when deploying platforms in semi-urban and rural areas	High	Medium	Deploy lightweight offline-first versions; partner with local telecoms for subsidised data; use solar charging points
3	Operational	Fieldwork access restricted in conflict-affected zones (e.g., North-West) for user testing and harm reporting	Medium	Medium	Phased coverage; partner with state governments; remote-first survey instruments and digital ethnography
4	Governance	Platform-COI perception (VigilSentinel, SPIDVerify, Wazobia) – stakeholders may view tools as government surveillance	Medium	Medium	Independent evaluation; IP assignment to FGN per ToR §11; published COI register; civil society oversight
5	User trust	Citizens distrust SPIDVerify identity verification and VigilSentinel harm reporting due to past NIMC data breaches	High	High	Co-design with civil society; publish transparency and breach-notification reports; offer offline verification and anonymous reporting channels
6	Operational	Researcher attrition (loss of trained data annotation and field staff)	Low	Medium	Over-recruitment buffer; cross-institution co-supervision; knowledge transfer workshops
7	Adoption (Wazobia)	Retailers resist switching to Wazobia Invoice due to perceived loss of cash transaction anonymity and unfamiliarity with digital receipts	Medium	Medium	Phased incentives (tax rebates); cooperative pilots before mandatory rollout; multilingual awareness campaigns
8	Legal	Cross-border transaction complaints (ECOWAS) fall outside Nigerian jurisdiction, limiting consumer redress	Medium	High	Partner with ECOWAS Commission; embed choice-of-law clauses; pilot a regional ombudsman for digital trade

A full risk register with probability/impact scores will be submitted in the Inception Report (Month 1).

8.5 Legislative Alignment by Sector

Table 13: Legislative alignment of research outputs across priority sectors and corresponding lead Ministries, Departments, and Agencies.

S/N	Sector	Key Legislation / Policy	Lead MDA
1	Banking	CBN Circular on Digital Financial Services (2023); BOFIA 2020; CBN Consumer Protection Regulations (31 January 2024)	CBN, FCCPC
2	Health	National Digital Health Strategy (2021–2025); NDPA 2023	Fed. Ministry of Health, NDPC
3	Defence	Cybercrimes Act 2015; National Cybersecurity Policy 2021	Office of NSA, Ministry of Defence
4	Regulation	NDPA 2023; Nigeria Startup Act 2022; NITDA Code of Practice (draft)	NDPC, NITDA, FMCIDE

Specific policy processes (e.g., NDPC guideline drafting Q4 2026, CBN circular revisions, NITDA Code consultations) are identified in the Policy Engagement Plan (Inception Report).

8.6 Ethics and Safeguards

All research complies with:

- NDPR (2019) and NDPA (2023),
- BUK Research Ethics Committee approval (IRB pre-fieldwork),
- World Bank ESS 2 on data privacy and vulnerable groups.

Safeguards include informed consent in local languages, anonymisation of harmful content datasets, child protection protocols (Stream 5), and mental health support for annotators. An independent ethics advisor (BUK Faculty of Law) will review protocols annually.

8.7 Cross-Cluster Coordination

Dr. Saratu Yusuf Ilu, current Head of the Department of Software Engineering at BUK, will serve as Cross-Cluster Coordinator. She holds a PhD in Computer Science from the African University of Science and Technology, Abuja (Distinction). With a strong record of multi-stakeholder coordination, research administration, and inclusive digital engagement – including her role as National Coordinator of the Digital Women Entrepreneurs Group – Dr. Ilu will work hand-in-hand with **Dr. Saminu Aliyu Kiri** (Programme Administrator) to oversee cross-cluster synthesis. Together, they will: (i) coordinate monthly meetings with the Quality Assurance Firm; (ii) manage anonymised

data sharing with Clusters B and F; (iii) ensure each research stream lead contributes timely inputs to joint policy briefs and national synthesis reports; and (iv) facilitate communication between the consortium’s Nigerian and international partners.

8.8 Impact Assessment Against Deliverables

Impact is embedded into every ToR deliverable: the **Inception Report** (Month 1) establishes the theory of change and results framework; **Quarterly and Annual Progress Reports** track policy citations, dataset use, and researcher milestones; the **Mid-Term Review** (Month 18) enables course correction; **Policy Briefs** are timed to specific MDA decision windows; and the **Final Report** (Month 36) delivers a consolidated impact statement including regulatory adoption, consumer harm reduction, and a sustainable researcher pipeline. Each deliverable functions as both a progress update and an impact verification point.

9 Eligibility Statement

All participating institutions satisfy the World Bank’s *Procurement Regulations for IPF Borrowers* (February 2025) regarding Conflict of Interest (paragraphs 3.15, 3.16), Un-fair Competitive Advantage (paragraph 3.17), and Eligibility (paragraphs 3.20–3.23). Supporting documentation accompanies this EOI.

Bayero University, Kano, the lead institution, is a Nigerian university eligible under the World Bank’s Procurement Regulations. All consortium members are accredited academic and research institutions with no known disqualifying conflicts.

10 Contribution to Project BRIDGE Objectives

Project BRIDGE is deploying at least 90,000 km of fibre-optic backbone. That will bring millions of Nigerians online, many for the first time. But infrastructure without knowledge is a road that leads to risk. Our research ensures connectivity and governance travel together.

- **Inclusive connectivity:** New users need safety and trust mechanisms from day one, not as an afterthought. Our work makes sure expanded connectivity protects all users, especially underserved communities.
- **Digital inclusion:** Trust barriers keep women, youth, persons with disabilities, and rural communities from fully joining the digital economy. We address those barriers with culturally grounded, linguistically diverse safety tools.
- **Economic transformation:** Digital commerce, fintech, and e-government need strong consumer protection. Our real-world platforms (Wazobia Invoice, VigilSentinel, SPIDVerify) prove that secure, locally designed digital solutions work.

- **National research capacity:** We're building a pathway from PhD candidate to postdoc to established professor in digital trust and safety. The goal: Nigeria producing the research that shapes its own digital future, not importing it. Our community networks extend this beyond formal academic institutions.
- **A replicable model:** This cluster integrates university research, industry platforms, and government policy expertise into a coordinated effort. Done well, it shows how future national research programmes can move beyond papers to real institutional change.

11 Conclusion

This consortium carries a record in exactly the areas Cluster E demands: hate speech detection, online safety, cybersecurity, trust systems, NLP for African languages, data privacy, AI governance, and digital identity. We've published at top venues, won major grants, built working platforms, and founded research communities. Those credentials are the entry ticket.

But the real test won't be measured in publications. It will show up in better policy. Stronger institutions. A more capable generation of Nigerian researchers. Research that turns into governance tools and safety mechanisms Nigerians can actually use.

That's what we're here to build. Academic research, industry platforms, and government policy experience, brought together into one research programme. Our aim: research findings that don't gather dust in journals but become the frameworks, regulations, and capabilities Nigeria needs as it builds one of Africa's most ambitious digital infrastructure programmes.

The countries that will lead in the decades ahead aren't just those that lay the most fibre. They're the ones that organise themselves to make connectivity safe, trusted, and inclusive. We're ready to help Nigeria be one of them.

12 Contact Information

Institution:	Bayero University, Kano
Contact Person:	Dr. Shamsuddeen Hassan Muhammad
Position:	Consortium Lead / Principal Investigator
Email:	shmuhammad.csc@buk.edu.ng
Phone:	08039647291
Web:	https://shmuhammadd.github.io

References

- [1] S. H. Muhammad, I. Abdulmumin, A. A. Ayele, D. I. Adelani, I. S. Ahmad, S. M. Aliyu, P. Röttger, et al., “AfriHate: A Multilingual Collection of Hate Speech and Abusive Language Datasets for African Languages,” in *Proceedings of NAACL 2025 (Volume 1: Long Papers)*, pp. 1854–1871, 2025.
- [2] S. M. Aliyu, G. M. Wajiga, M. Murtala, S. H. Muhammad, I. Abdulmumin, and I. S. Ahmad, “HERDPhobia: A Dataset for Hate Speech against Fulani in Nigeria,” *arXiv preprint arXiv:2211.15262*, 2022.
- [3] S. H. Muhammad, I. Abdulmumin, A. A. Ayele, N. Ousidhoum, D. I. Adelani, et al., “AfriSenti: A Twitter Sentiment Analysis Benchmark for African Languages,” in *Proceedings of EMNLP 2023*, 2023.
- [4] S. H. Muhammad, D. I. Adelani, S. Ruder, I. S. Ahmad, I. Abdulmumin, et al., “NaijaSenti: A Nigerian Twitter Sentiment Corpus for Multilingual Sentiment Analysis,” in *Proceedings of LREC 2022*, 2022.
- [5] S. H. Muhammad, D. I. Adelani, S. Ruder, I. S. Ahmad, I. Abdulmumin, B. S. Bello, M. Choudhury, C. C. Emezue, S. S. Abdullahi, A. Aremu, et al., “NaijaSenti: A Nigerian Twitter Sentiment Corpus for Multilingual Sentiment Analysis,” in *Proceedings of the Thirteenth Language Resources and Evaluation Conference (LREC 2022)*, pp. 590–602, European Language Resources Association, 2022.
- [6] U. Naseem, R. Geislinger, J. Ren, S. Kohail, R. G. Veliz, P. S. Sahil, Y. Zhang, M. A. Stranisci, I. Abdulmumin, Ö. Alacam, C. Acarturk, A. Jabr, S. Anwar, A. A. Ayele, S. Frenda, A. T. Cignarella, E. Tutubalina, O. Rogov, A. K. Htet, X. Wang, S. Thapa, K. Rauniyar, T. Chakraborty, A. Zeeshan, D. Kodati, S. Keerthi, S. Moradizyev, F. Alam, A. Hasan, S. I. Ahmed, Y. K. Thu, S. Parida, I. A. Qazi, L. Wanzare, N. O. Onyango, C. Siro, J. W. Kimani, I. S. Ahmad, A. C. Ali, M. Semmann, C. Biemann, S. H. Muhammad, and S. M. Yimam, “POLAR: A Benchmark for Multilingual, Multicultural, and Multi-Event Online Polarization,” *arXiv preprint arXiv:2505.20624*, 2026.
- [7] A. B. Usman and J. A. Gutiérrez, “Toward trust based protocols in a pervasive and mobile computing environment: A survey,” *Ad Hoc Networks*, vol. 81, pp. 143–159, 2018.
- [8] A. B. Usman and J. A. Gutiérrez, “DATM: a dynamic attribute trust model for efficient collaborative routing,” *Annals of Operations Research*, vol. 277, no. 2, pp. 293–310, 2019.
- [9] A. Wells and A. B. Usman, “Trust and Voice Biometrics Authentication for Internet of Things,” *International Journal of Information Security and Privacy*, vol. 17, no. 1, pp. 1–28, 2023.

- [10] A. Wells and A. B. Usman, "Privacy and biometrics for smart healthcare systems: attacks, and techniques," *Information Security Journal: A Global Perspective*, vol. 33, no. 3, pp. 307–331, 2024.
- [11] A. Wells, N. Dajnowski, A. B. Usman, J. Murray, and B. Barakat, "Privacy-Enhanced One-to-Many Biometric System Using Smart Contracts: A New Framework," in *2024 29th International Conference on Automation and Computing (ICAC)*, pp. 1–6, 2024.
- [12] I. Abdulmumin and B. S. Galadanci, "hauWE: Hausa Words Embedding for Natural Language Processing," in *Proceedings of IEEE Nigeria Computer Conference*, pp. 1–6, 2019.
- [13] I. Abdulmumin and V. Marivate, "ZASCA-Sum: A Dataset of the South Africa Supreme Courts of Appeal Judgments and Media Summaries for Legal Documents Summarization Research," *Data in Brief*, 2025.
- [14] A. A. Bisu, A. Gallant, and H. Sun, "HYBIC: An Improved Congestion Control Algorithm for Integrated Satellite-Terrestrial Networks in 5G and Beyond Communications," in *Proceedings of the 2024 IEEE Future Networks World Forum (FNWF)*, Dubai, UAE, 2024.
- [15] A. Fraser, A.-S. Shehu, N. Frymann, P. Haynes, and S. Schneider, "Privacy-Preserving Photo Sharing: An SSI Use Case," in *Information Systems Security, ICISS 2024, Lecture Notes in Computer Science*, vol. 15416, pp. 320–329, Springer, 2025.
- [16] A.-S. Shehu and S. Schneider, "Decentralised supply chain reputation: A privacy and self-sovereign identity perspective," in *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 474–484, 2024.
- [17] A.-S. Shehu, A. Pinto, and M. E. Correia, "SPIDVerify: A secure and privacy-preserving decentralised identity verification framework," in *2023 International Conference on Smart Applications, Communications and Networking (SmartNets)*, pp. 1–8, IEEE, 2023.
- [18] S. M. Abdulrahman, P. Brazdil, J. N. van Rijn, and J. Vanschoren, "Speeding up algorithm selection using average ranking and active testing by introducing runtime," *Machine Learning*, vol. 107, no. 1, pp. 79–108, 2018.
- [19] S. Abubakar, A. A. Bichi, S. M. Abdulrahman, and I. S. Ahmad, "A multi-task learning framework for sentiment analysis and news classification for low-resource language," *Journal of Basics and Applied Sciences Research*, vol. 4, no. 2, pp. 233–242, 2026.

- [20] K. Haruna, M. A. Ismail, A. Qazi, H. A. Kakudi, M. Hassan, S. A. Muaz, and H. Chiroma, "Research paper recommender system based on public contextual metadata," *Scientometrics*, pp. 1–14, 2020.
- [21] T. M. Ibrahim, H. Chiroma, S. i. M. Abdulhamid, M. A. Al-garadi, N. Rana, A. N. Muhammad, and K. Haruna, "Recent advances on mobile touch screen security authentication methods: A systematic literature review," *Computers and Security*, 2018.
- [22] M. Ibrahim, A. Abdullahi, A. Adamu, A. U. Jibril, and K. Haruna, "Survey on literatures for the detection of android malware using machine learning," *BIMA Journal of Science and Technology*, vol. 7, no. 01, pp. 333–361, 2023.
- [23] I. S. Ahmad, S. Dudy, R. Ramachandranpillai, and K. Church, "Are generative language models multicultural? A study on Hausa culture and emotions using ChatGPT," in *Proceedings of the 2nd Workshop on Cross-Cultural Considerations in NLP (C3NLP)*, pp. 98–106, Association for Computational Linguistics, 2024.
- [24] I. S. Ahmad, L. J. Aliyu, A. A. Khalid, S. M. Aliyu, S. H. Muhammad, I. Abdulmumin, et al., "Analyzing COVID-19 vaccination sentiments in Nigerian cyberspace: Insights from a manually annotated Twitter dataset," arXiv preprint arXiv:2401.13133, 2024.
- [25] A. G. Sharifai and Z. Zainol, "Multiple Filter-Based Rankers to guide Hybrid Grasshopper Optimisation Algorithm and Simulated Annealing for Feature Selection," *IEEE Access*, vol. 9, pp. 74127–74142, 2021.
- [26] M. Danlami, I. B. Bakari, A. G. Sharifai, and U. S. Haruna, "Focal Loss and Self-Attention Convolutional Neural Network for Phishing Detection," in *2024 1st International Conference on Cyber Security and Computing (CyberComp)*, pp. 1–6, IEEE, 2024.
- [27] Lacuna Fund. *Lacuna Fund 2021 Language Datasets Award — Development of Hate Speech Dataset for African Languages (AfriHate)*. 2022. URL: <https://lacunafund.org/2021-african-language-awardees/>.
- [28] University of Surrey. *Centre for the Decentralised Digital Economy (DECaDE)*. 2020. URL: <https://decade.ac.uk/>. Funding: £10 million from UK Research & Innovation (UKRI) through the Digital Economy Programme (EPSRC) and industrial partners.
- [29] CINTESIS. *NanoSTIMA - Macro-to-Nano Human Sensing: Towards Integrated Multimodal Health Monitoring and Analytics*. 2023. URL: <https://cintesis.eu/pt/portfolio-items/nanostima/>. Funding: NORTE-01-0145-FEDER-000016.
- [30] The Condia. *Nigeria awards AI research grant to Lendsqr and 44 other startups and experts*. November 26, 2024. URL: <https://thecondia.com/>

[nairs-grantee-ai-research-grantee/](#). Note: Part of the debut National AI Research Scheme (NAIRS) by Nigeria’s Federal Ministry of Communications, Innovation & Digital Economy. Each grantee received a ₦5 million grant

- [31] U. S. Haruna, A. A. Mahmoud, M. Danlami, and A. G. Sharifai, “Enhancing Network Intrusion Detection with Hybrid Deep Learning: SWIN Transformer and VGG19,” in *2024 1st International Conference on Cyber Security and Computing (CyberComp)*, pp. 13–18, IEEE, 2024.

Glossary of Acronyms

AI	Artificial Intelligence
ADUSTA	Aliko Dangote University of Science and Technology
AML	Anti-Money Laundering
BOFIA	Banks and Other Financial Institutions Act (2020)
BRIDGE	Building Resilient Digital Infrastructure for Growth (Project)
BUK	Bayero University, Kano
CBN	Central Bank of Nigeria
CC-BY	Creative Commons Attribution License
CIT	Centre for Information Technology
CSV	Comma-Separated Values
CV	Computer Vision
DECaDE	Centre for the Decentralised Digital Economy
DOI	Digital Object Identifier
DSA	Digital Services Act (EU)
ECOWAS	Economic Community of West African States
EHR	Electronic Health Record
EOI	Expression of Interest
ESS	Environmental and Social Standard (World Bank)
EU	European Union
FCCPA	Federal Competition and Consumer Protection Act (2018)
FCCPC	Federal Competition and Consumer Protection Commission
FMCIDE	Federal Ministry of Communications, Innovation and Digital Economy
FUT Babura	Federal University of Technology, Babura
GDPR	General Data Protection Regulation (EU)
GPU	Graphics Processing Unit
HCI	Human-Computer Interaction
ICT	Information and Communications Technology
IdMAI	Identity Management and Authorization Infrastructure
ILP	Inductive Logic Programming
INEC	Independent National Electoral Commission
IoT	Internet of Things

IRB	Institutional Review Board
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
JV	Joint Venture
KYC	Know Your Customer
ADUST	Kano University of Science and Technology, Wudil
LLM	Large Language Model
M2M	Machine-to-Machine
MDA	Ministry, Department or Agency
MPC	Multi-Party Computation
NAACL	North American Chapter of the Association for Computational Linguistics
NAIRS	National AI Research Scheme (Nigeria)
NCC	Nigerian Communications Commission
NDPA	Nigeria Data Protection Act (2023)
NDPC	Nigeria Data Protection Commission
NDPR	Nigeria Data Protection Regulation (2019)
NIMC	National Identity Management Commission
NIN	National Identification Number
NIPSS	National Institute for Policy and Strategic Studies (Nigeria)
NITDA	National Information Technology Development Agency
NLP	Natural Language Processing
NSA	National Security Adviser (Office of)
ONSA	Office of the National Security Adviser
PWDs	Persons with Disabilities
QA	Quality Assurance
QCBS	Quality- and Cost-Based Selection
REF	Research Excellence Framework (UK)
RIS3	Research and Innovation Strategy for Smart Specialisation
SaaS	Software as a Service
SPIDVerify	Secure, Privacy-preserving Identity Verification (platform)
SSI	Self-Sovereign Identity
ToR	Terms of Reference
UBEC	Universal Basic Education Commission (Nigeria)
UK	United Kingdom
WP	Work Package