



Co-creation HUB



CcHUB
DESIGN
LAB

PROTECTING LEARNERS IN THE DIGITAL AGE

The State of Child Safeguarding in
Kenya and Nigeria's EdTech Ecosystems



About Co-Creation Hub Design Lab



Co-creation Hub Design Lab is a research and development laboratory innovating for social impact. We collaborate with global stakeholders to explore the application of technology to solve Africa's systemic challenges in public health, education, creative Industries, governance, and the private sector.

Our approach is centred on people being at the heart of every intervention. We move beyond designing for users by partnering with them throughout the entire process. From initial concepts to testing and prototyping, users are active contributors rather than passive recipients. This human-centric approach guides our efforts to solve complex problems that have a meaningful impact on individuals and communities. We define design excellence as the successful fusion of creative innovation with substantial social value.

Contact us
Co-creation Hub
First floor, Golden Plaza
KG 546 St.1 Kamatamu, Kacyiru Kigali, Rwanda

T: +250 787 830 300
E: designlab@cchub.africa
W: www.cchubnigeria.com/designlab

Authors

Movine Omondi
Moses Kioko
Maxwel Cheruiyot
Fredrick Mwangangi

Editors

George Bush Otieno
Joy Matheka

June 2026



Table of Content

About Co-Creation Hub Design Lab

Abstract	1
Key Findings	2
1. Introduction	3
2. Safeguarding Landscape Analysis	4
2.1 Overview of Safeguarding Practice in Africa se Rates	4
2.2 Child Safeguarding in Kenya and Nigeria	6
2.3 Child Safeguarding in Education Technology (Edtech)	7
3. Landscape of Safeguarding in Education Technology in Kenya and Nigeria	7
3.1 Institutional Framework and Policy Adoption	8
o 3.1.1 Safeguarding Policies	8
o 3.1.2 Safety by Design	9
3.2 Risk Management and Monitoring	10
o 3.2.1 Risk Strategy	10
3.3 Organizational Capacity and Accountability	10
o 3.3.1 Safeguarding and Staff Capacity	10
o 3.3.2 Safeguarding Risk Registers	11
o 3.3.3 Safeguarding Risk Assessment	12
3.4 User Reporting and Feedback Mechanisms	12
o 3.4.1 Reporting Mechanisms	12

3.5 Data Privacy and Information Security	13
o 3.5.1 Data Management	13
3.6 Inclusive Safety and Accessibility	14
o 3.6.1 Safety Features	14
o 3.6.2 Inclusive Reporting	14
3.7 Content Moderation and Protective Controls	15
o 3.7.1 Behaviour Guidelines	16
o 3.7.2 Safeguarding Contact	16
o 3.7.3 Data Privacy	16
o 3.7.4 Complaint Mechanism	17
o 3.7.5 Blocking Features	18
o 3.7.6 Inclusive Safety	18
o 3.7.7 Accessibility Check	19
o 3.7.8 Feedback Linkage	20
o 3.7.9 Child-Friendly Terms	20
o 3.7.10 Third Parties	21
o 3.7.11 Contracts & Compliance	21
o 3.7.12 Parental Controls	22
o 3.7.13 Content Filtering	22
3.8 Product and Platform Safety Reviews	23
o 3.8.2 Tool Safety Review	23
o 3.8.3 Platform Safety Review	24
4. Emerging Global Safeguarding Trends	24

o 4.1 Safeguarding Publication Trends	25
o 4.2 Data Privacy Concerns	25
4.3 Data Protection and Privacy Systems	26
4.4 Potential Privacy Risks	28
4.5 Safeguarding Safety Features	28
4.6 Key Thematic Areas	28
5. Ecosystem-Level Insights and Implications	29
5.1 Safeguarding as a Strategic Priority	30
5.2 Safeguarding Fatigue Across Cohorts	30
5.3 Weak Training Culture	30
5.4 Inclusion and Accessibility Gaps	30
5.5 Data Management as a Strength to Build On	31
5.6 Governance and Accountability Weaknesses	31
5.7 Fragmented Safety Reviews	31
5.8 Towards a Collaborative Ecosystem	31
6. Conclusion	32
7. Recommendations	33
o 7.1 For EdTech Startups	33
o 7.2 For Accelerators and Funders	34
o 7.3 For the Broader Ecosystem	35
8. References	35

Abstract

The integration of digital technologies in education, otherwise known as education technology (Edtech), enhances learning outcomes for many learners. Digital learning accelerated sharply during the COVID-19 pandemic. However, despite achieving notable milestones, this rapid shift also introduced safeguarding risks that warrant attention.

For instance, EdTech products that are not designed with children's rights and contextualised safety needs in mind expose young learners and other vulnerable users to a range of safeguarding harms. Data privacy risks, inadequate reporting mechanisms, insufficient behavioural guidelines, and gaps in instructor awareness can create an environment in which children may not consistently receive the protection they need when engaging with digital learning tools.

Our study is based on implementation data from the Mastercard Foundation EdTech Fellowship Programme, a Pan-African Edtech innovation initiative supported by the Mastercard Foundation, with operations in Kenya and Nigeria. The analysis covers 59 startups from the three initial cohorts in the programme across Nigeria and Kenya. It is also enriched by secondary sources encompassing at least 603 peer-reviewed articles and technical reports, safeguarding priorities.

thus providing a comprehensive and grounded landscape analysis of emerging trends in safeguarding within the Edtech industry, e.g., data privacy concerns and thematic

The study reveals a consistent pattern: while many startups demonstrate commitment to safeguarding practices, notable adoption gaps persist. Critical challenges include deteriorating inclusive design practices, weak organisational training cultures, and near-absent safeguarding risk registers, all of which point to 'safeguarding fatigue', a gradual deprioritisation of child protection as business pressures escalate.

At the same time, there are genuine strengths to build on. Content review processes, data management policies, and feedback linkage mechanisms show relatively strong and consistent adoption. These areas offer a foundation for revitalising a more robust, sector-wide safeguarding culture.

Priority recommendations include: integrating safeguarding standards in product development, mandating compulsory safeguarding training for Edtech product designers and engineers, and linking safeguarding outcomes to progress markers in investment rounds. Still, achieving lasting progress necessitates a coordinated strategy across the wider Edtech ecosystem and the education sector as a whole, from startups and teachers to investors, regulatory agencies, and ministries of education.

Key Findings

01

Diverse Target Demographics. More than half (53.6%) of EdTech startups in Kenya primarily serve children under 18. Nigerian startups serve a broader mix: 34.5% target adults, and a further 34.5% serve both children and young people.

02

Policy vs. Practice Gap. Safeguarding policies exist in both countries, but implementation is inconsistent. Kenya's Cohort 2 reached 86% policy adoption, while Cohort 3 fell sharply to just 40%. Nigeria started at 100% in Cohort 1, declined to 45% in Cohort 2, and recovered to 62% in Cohort 3.

03

Risk Management Gaps. Risk registers are virtually absent in Kenya and Nigeria, both of which recorded 0% by Cohort 3. Safeguarding risk assessment followed a steep downward trajectory: Kenya dropped from 50% in Cohort 1 to 0% in Cohort 3; Nigeria fell from 50% to just 14%.

04

Safeguarding Strengths. Content review stood out as a consistently strong area, with 86%–100% adoption in earlier cohorts across both countries. Data management policy adoption was similarly high, reaching 100% in Nigeria's Cohort 3.

05

Decline in Inclusive Design. Inclusive safety in Kenya fell from 100% in Cohort 1 to just 20% in Cohort 3. Accessibility checks reached 0% in Kenya and only 20% in Nigeria by the third cohort.

05

Weak User Protection Features. Parental controls fell from 57% to 0% across cohorts in Kenya. Content filtering adoption remained below 50% in both countries throughout the study period.

1.0 Introduction



This study examines the state of safeguarding in EdTech products across Kenya and Nigeria. The analysis draws on project implementation data from startups in the Mastercard Foundation EdTech Fellowship Programme, as well as a meta-analysis of 603 safeguarding publications, to situate those findings within broader global and continental trends.

To evaluate various safeguarding focal areas, secondary sources were collected via Google, cleaned, and synthesised using a Large Language Model (LLM) for summarisation and zero-shot classification. Feature extraction was employed to capture document metadata, including titles, publication dates, and authors, as well as referenced countries and key thematic domains such as data protection protocols, safeguarding features, privacy concerns, and potential risks.

The goals of this research are three-pronged. It seeks to identify global trends in the safeguarding of children and at-risk adults, and evaluate safeguarding practices across existing and past EdTech initiatives to detect critical deficiencies. Finally, it seeks to provide actionable recommendations to close emerging gaps, strengthen support for the startup community, and foster a robust culture of safeguarding excellence in educational technology solutions.

2.0 Safeguarding Landscape Analysis

2.1 Overview of Safeguarding Practice in Africa



Safeguarding refers to the organisational efforts, mandates, and commitment required to prevent and respond effectively to risks that may harm children, young people, and vulnerable adults ([Chambers et al., 2021](#); [UNICEF, 2026](#)). In practice, robust safeguarding requires organisations to intentionally integrate care and take responsibility for doing no harm across all aspects of their operations and initiatives ([UNHCR, 2002](#)). While closely related to child protection, the activities that involve protecting children from all forms of abuse, exploitation, and neglect, they differ in scope ([Johnson & Sloth-Nielsen, 2020](#)). While child protection implies a wider mandate typically spearheaded by governmental and intergovernmental entities, safeguarding brings responsibility closer to organisations.

Globally, the prominence of safeguarding was largely elevated by high-profile scandals involving both commercial and non-profit organisations. A particularly influential case was the Oxfam scandal, in which systemic sexual abuses by staff against earthquake victims in Haiti came to light, prompting a fundamental re-examination of safeguarding obligations across the development and humanitarian sector. At the continental level, the African Charter on the Rights and Welfare of the Child ([the African Children's Charter](#)) is the primary framework that guides child protection and safeguarding practice.

Additionally, the African Children's Committee in its 2018 analysis, directly addressed the centrality of child safeguarding for the first time, urging state parties to ensure that all civil society organisations and international organisations

working with children adopt formal child safeguarding policies and that individuals with histories of child abuse be prevented from being involved with children, even as volunteers ([ACERWC, 2018](#)).

The Committee also adopted Africa's Agenda for Children 2040, a critical component of the African Union's Agenda 2063, which calls for stakeholder collaboration to prevent sexual abuse by workers of development agencies, and for all entities working with children to establish both child protection and safeguarding policies ([ACERWC, 2018](#)).

While child protection has historically been the primary concern for most developmental and humanitarian actors, other key areas now emerging within the safeguarding frame include gender-based violence, data protection, workplace safety, and digital safety ([Grant, 2026](#)).



2.2 Child Safeguarding in Kenya and Nigeria

Kenya's and Nigeria's safeguarding landscapes entail complex interactions among actors and networks. In Kenya, the government has progressively put in place critical legislative and policy frameworks, including the Children Act (2022), the Sexual Offences Act, the Computer Misuse and Cybercrimes Act (2019), and the Data Protection Act (2019). Despite this, implementation remains incomplete. Research points to the need to fast-track child safeguarding and protection efforts by building relevant technical capacity and funding.

Nigeria's child safeguarding framework shows a relatively advanced stage of development, anchored by the Child Rights Act (2003), the Violence Against Persons (Prohibition) Act (2015), and the Cyber Crimes Act (2015). However, comparative analyses have highlighted the need for Nigeria to strengthen practical response mechanisms, including sex offender treatment and prevention programmes, effective enforcement, and more comprehensive data collection on the state of child protection. Advocacy, awareness, and education on children's rights are also widely seen as essential complements to legislative activity.



2.3 Child Safeguarding in Education Technology (Edtech)

As a result of the significant and lasting influence of educational technology (Edtech) on students and the ongoing need to gather personal data, safeguarding is not just a functional requirement; it is a pivotal moral and ethical necessity. Thus, all stakeholders involved in providing Edtech tools to students, including learning institutions, educators, technology providers, governments, and development partners, must centre students' safety, digital health, and data privacy as fundamental, non-negotiable pillars of EdTech integration.

A socio-legal analysis of data governance in the United Kingdom found key inefficiencies in schools' capacity to hold EdTech companies accountable for the ethical collection and processing of student data([Day et al., 2022](#)).

The study underlined the need for schools and other parties handling student data to align their work with children's rights, statutory safeguarding requirements, and educational needs, a lesson that is equally applicable to the African context.

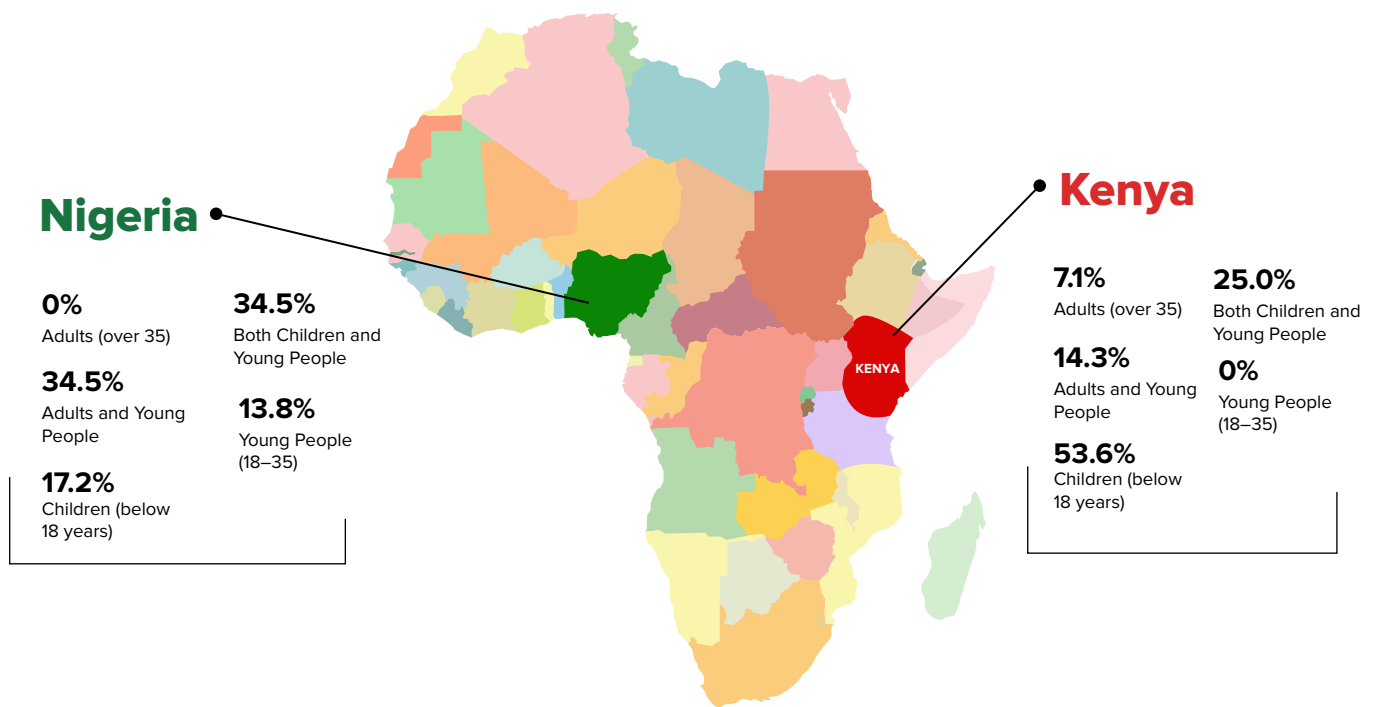
It is also key to recognise that many EdTech products and services are often not inherently designed with children's rights in mind or with contextualised safety-by-design strategies. These gaps mean that the very platforms meant to democratise learning can inadvertently expose young users to harm. Stakeholders who promote, design, and implement EdTech solutions, therefore, bear a responsibility to ensure that these tools are both inclusive and safe.

3.0 Landscape of Safeguarding in Education Technology in Kenya and Nigeria

Data from the initial cohorts of the Mastercard Edtech Fellowship Programme highlights distinct user demographics across the two regions.

- In Kenya, children under 18 make up the majority of Edtech product users at 53.6%, whereas in Nigeria, this group accounts for only 17.2%.
- Startup targeting strategies also varied by country. Nigeria has startups specifically focusing on young people under 35, who make up 13.8% of their total user base. At the same time, Kenya featured products expressly designed for adults over 35, accounting for 7.1% of its Edtech solutions.

As such, while both countries offer products for diverse demographics, Nigerian startups generally provide services across a broader age spectrum. Specifically, Nigerian beneficiary groups for 'Adults and Young People' and 'Both Children and Young People' each represent 34.5% of the market. In contrast, Kenyan startups maintain a sharper focus on younger users, with 25% of their beneficiary base comprising both children and young people combined. Consequently, while Kenyan Edtech remains heavily focused on children, Nigerian startups are reaching a broader range of age groups, including older adults.



3.1 Institutional Framework and Policy Adoption

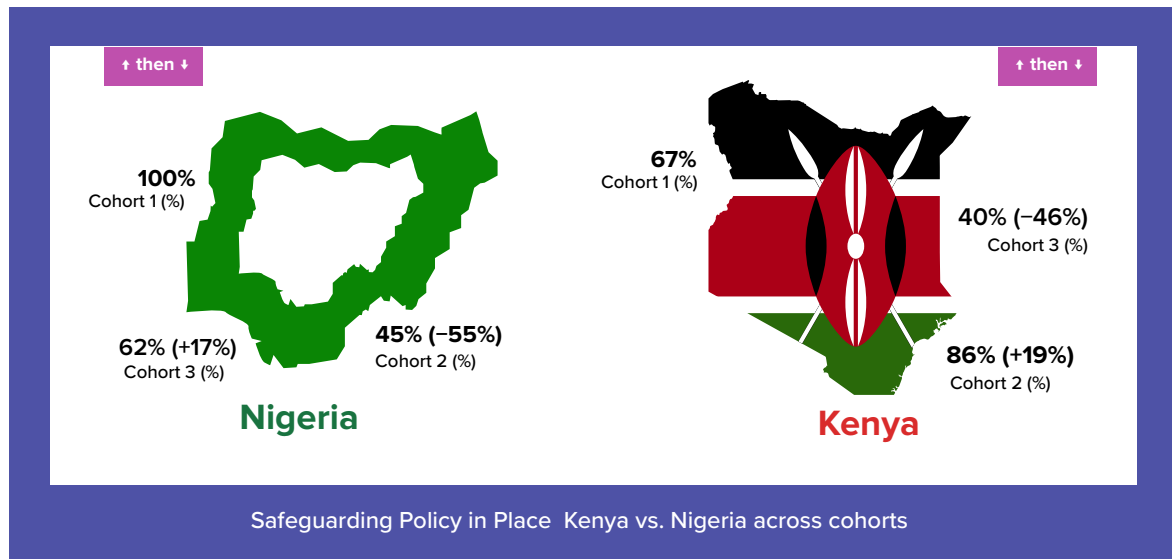
3.1.1 Safeguarding Policies

Kenya's child safeguarding obligations are grounded in the Constitution (Article 53) and the Children Act 2022. Nigeria's equivalent framework is the Child Rights Act 2003. Both provide important foundations for protecting children from abuse, neglect, exploitation, and harmful practices. The use of safeguarding policies by Edtech startups varies across the countries and cohorts.

For instance, 67% of Kenyan startups in cohort 1 had safeguarding policies, a figure that rose by 19% to 86% in cohort 2 and declined sharply to just 40% for cohort 3. Similarly, Nigerian startups also had stronger integration of safeguarding policies in earlier cohorts: 100% in Cohort 1, dropping to 45% in Cohort 2, and increasing to 62% in Cohort 3.

Both countries experienced a decline in the utilisation of safeguarding policies from the first cohort, although Kenya's landscape shows a sustained regression, while Nigeria's shows a mixed picture and resilience. The volatility across cohorts signals that safeguarding policy adoption cannot be taken for granted.

The state of decline in integration of safeguarding practice is particularly concerning, given the increasingly child-centred nature of many Kenyan Edtech products, and requires urgent intervention, mandatory safeguarding, and child-protection training for all Edtech startups, as well as periodic refresher sessions. This will ensure that staff have the competencies needed to apply safeguarding policies in daily operations and in digital product design.



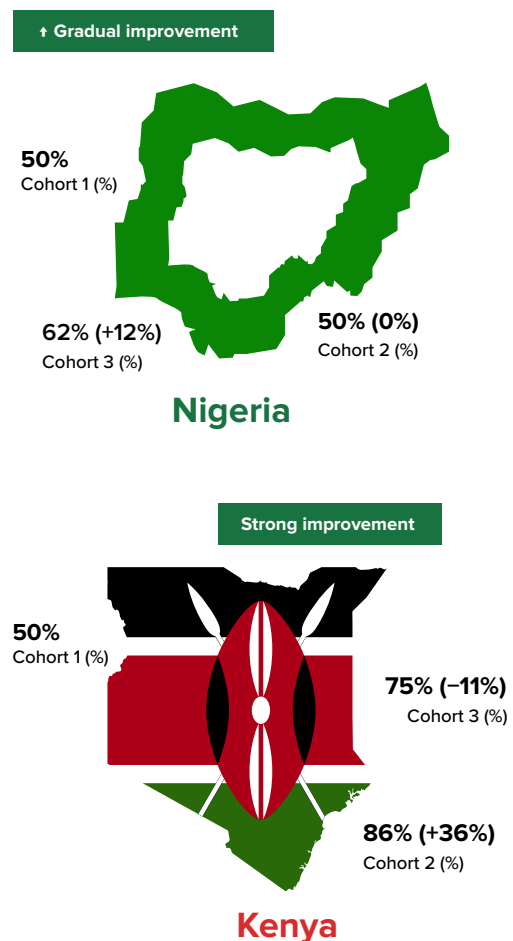
3.1.2 Safety by Design

Safety by design is a preventive approach that prioritises user safety by identifying and mitigating potential risks throughout the product development process. EdTech startups are expected to anticipate, detect, and eliminate online harms before they occur, rather than react to them after the fact.

Kenyan startups demonstrate stronger safety-by-design capacity, with 86% and 75% of startups in cohorts 2 and 3, respectively, having some safety-by-design measures in place. Nigerian startups have a more modest capacity, 62% in cohort 3, albeit a consistent growth has been experienced.

To maintain this rather positive trajectory, Edtech startups need to institutionalise continuous safety-by-design audits and establish a

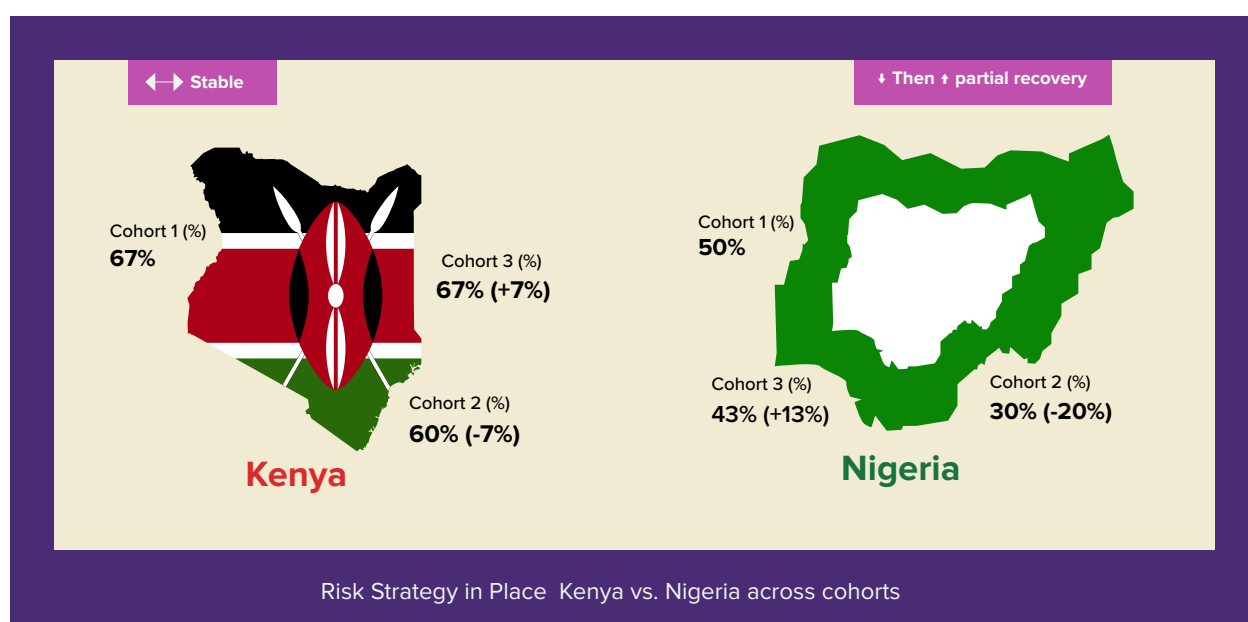
monitoring framework that proactively identifies and mitigates child-specific online risks, in line with national child-safety laws.



3.2 Risk Management and Monitoring

A safeguarding risk strategy enables organisations to identify, assess, mitigate, and monitor risks that could harm learners. For EdTech platforms operating at scale, a clearly articulated risk strategy is critical; it is a core safeguarding obligation. Kenyan startups maintain a stronger risk strategy integration, with 67% of startups in both cohort 1 and cohort 2 of the programme having established frameworks. Nigerian startups have 50% integration in cohort 1 and 43% in cohort 3, with just 30% in cohort 2.

3.2.1 Risk Strategy

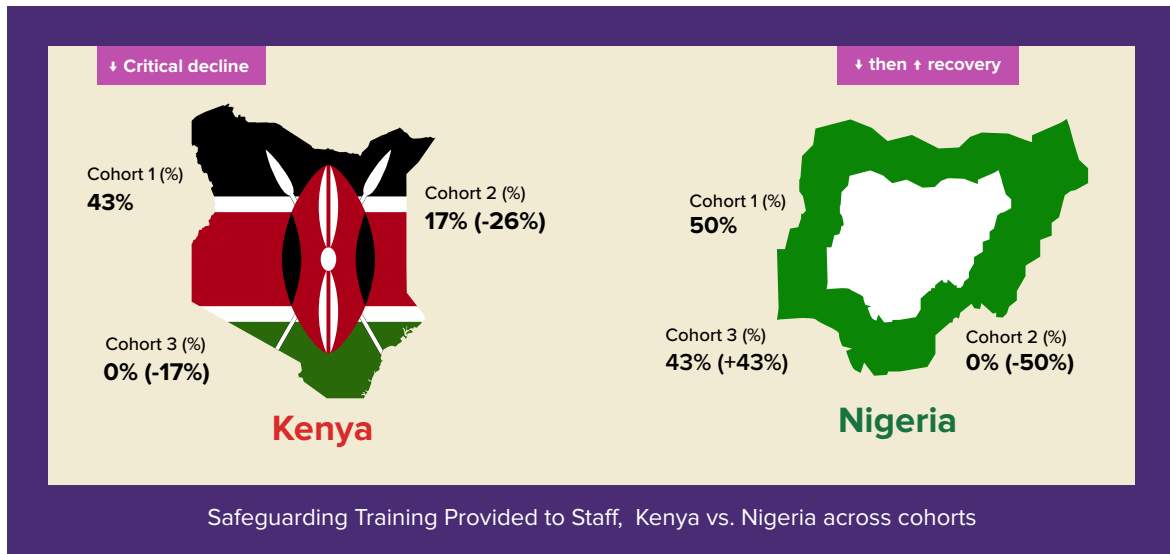


3.3 Organizational Capacity and Accountability

3.3.1 Safeguarding and Staff Capacity

Training staff on child protection enables them to recognise, prevent, and respond to risks of harm, abuse, or exploitation on their platforms. It is one of the most effective techniques of translating policy into practice, and one of the areas showing the most alarming decline.

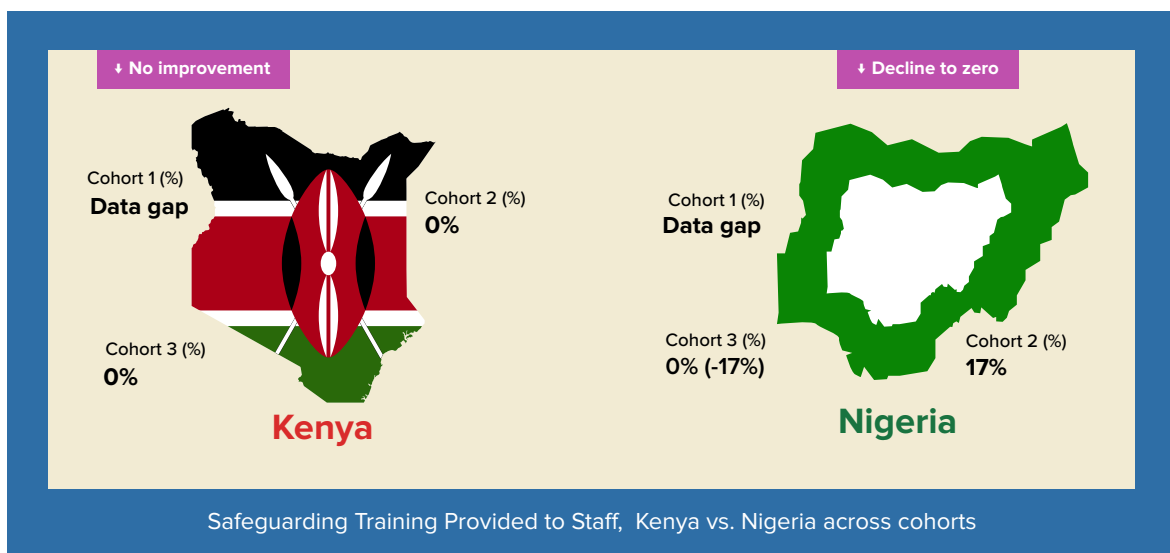
In Kenya, 43% of Cohort 1 startups had trained their staff, a reasonable starting point. A trend that fell in Cohort 2 (-26%) and declined further in Cohort 3 (-17%). In Nigeria, the safeguarding training rate was 50% in Cohort 1, yet no Nigerian startup provided it in Cohort 2. Cohort 3 saw a recovery to 43%. Safeguarding training should be a precondition for deploying Edtech platforms to learners.



3.3.2 Safeguarding Risk Registers

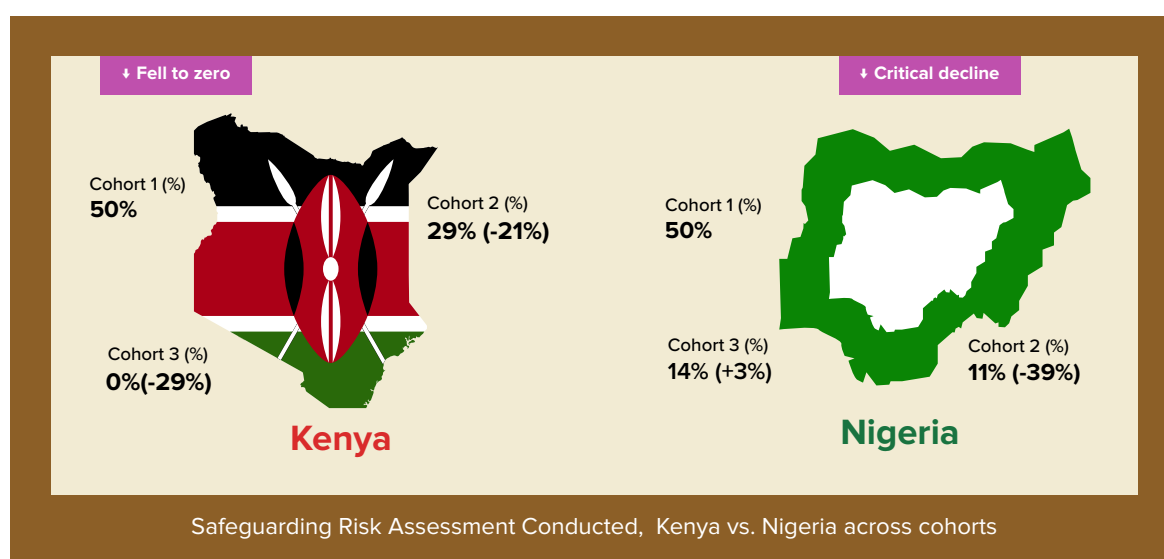
A safeguarding risk register is a practical management tool used to document, track, and minimise potential safeguarding risks to children and vulnerable people. Despite its importance, it is the area where both countries show the most consistent weakness.

In Kenya, no startup in both Cohort 2 and Cohort 3 maintained an updated risk register. In Nigeria, only 17% of Cohort 2 startups had one, but none in Cohort 3 did. Data was not available for Cohort 1 in either country. The limited existence of risk registers across the cohorts raises serious concerns about how safeguarding incidents are documented and how risks are tracked over time.



3.3.3 Safeguarding Risk Assessment

EdTech startups must identify, assess, and respond to safeguarding risks affecting children and young people. Risk assessments should cover both organisational activities and the products and services being delivered to learners. Both countries demonstrated a sharp downturn in safeguarding risk assessments by the third cohort. Kenya, which initially reported a 50% adoption rate in Cohort 1, saw a 21% decrease in Cohort 2 with no reported risk assessment in Cohort 3. Nigeria followed a comparable path, starting at 50% and experiencing a notable 39% decline in Cohort 2, with only a slight recovery to 14% by Cohort 3. Consequently, by the conclusion of the study period, startups in both regions have largely ceased performing these essential assessments.

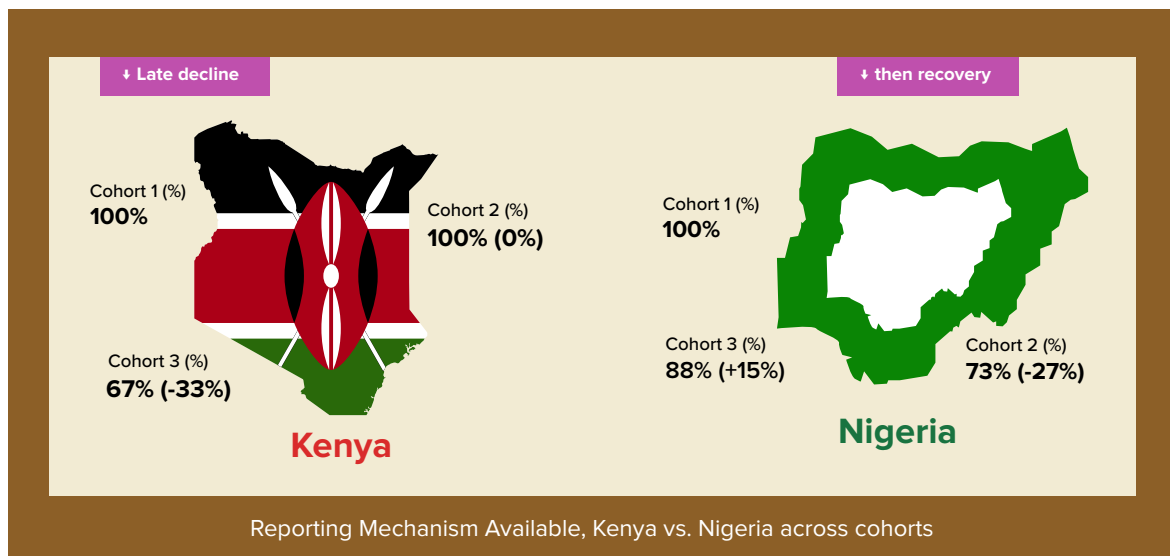


3.4 User Reporting and Feedback Mechanisms

3.4.1 Reporting Mechanisms

Reporting mechanisms allow platform users to raise concerns about harm, exploitation, and abuse safely and confidentially. They are among the most fundamental safeguarding features any EdTech product can embed. This is one of the stronger areas across both countries. Kenya maintained 100% implementation in Cohorts 1 and 2, with a decline to 67% in Cohort 3, still above average. Nigeria also started at 100% in Cohort 1, fell by (-27%) in Cohort 2, and recovered to 88% in Cohort 3. Both countries demonstrate a relatively sustained commitment to making reporting available, though there is room to strengthen the quality and inclusivity of those mechanisms.

All startups should implement confidential, child-friendly, and disability-inclusive reporting systems with clear response timelines and feedback procedures, ensuring every learner can safely raise concerns without fear of retaliation.

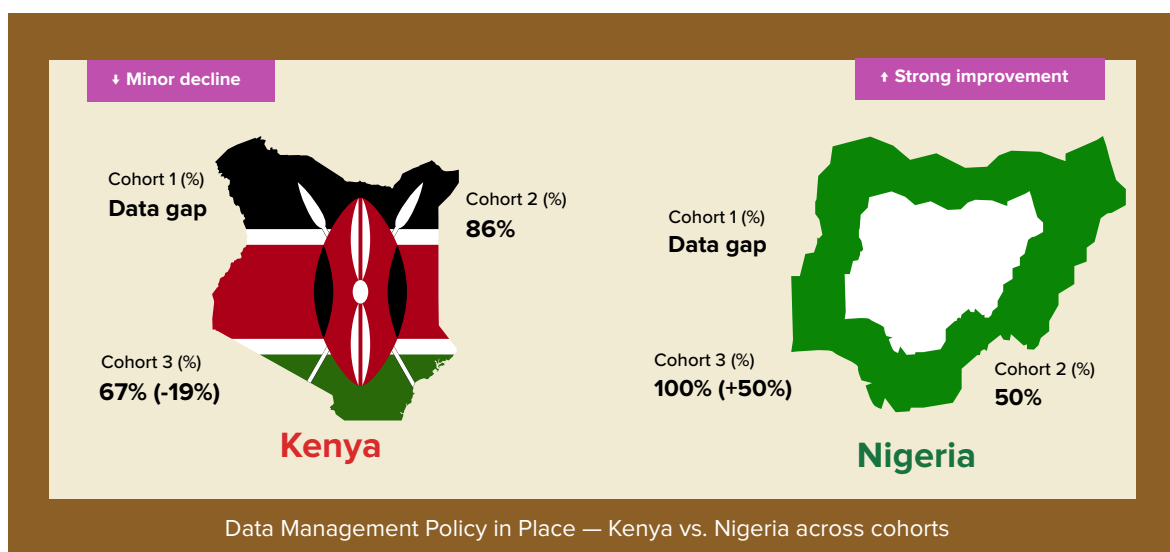


3.5 Data Privacy and Information Security

3.5.1 Data Management

Data management is also one of the programme's strongest areas. In Kenya, 86% of Cohort 2 startups had a data management policy, though the figure dropped to 67% in Cohort 3, still above average. While in Nigeria, 50% of Cohort 2 had data management systems, with Cohort 3 startups achieving 100% adoption. Therefore, despite data gaps in Cohort 1 for both countries, more than half of the startups in subsequent cohorts had data management practices in place.

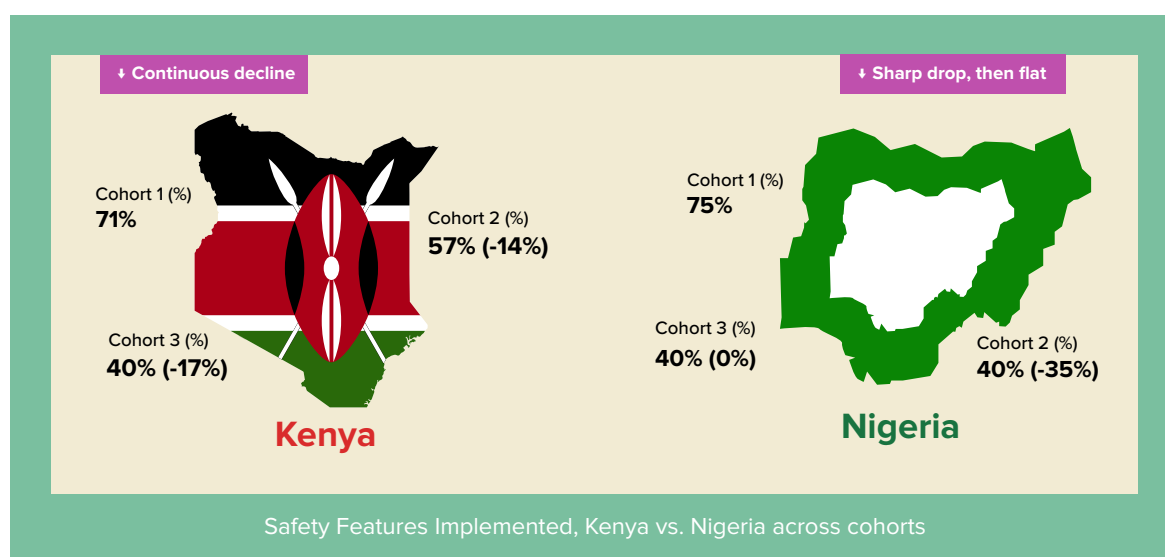
EdTech startups have a responsibility to maintain secure storage for learner information and ensure that any data sharing is conducted under transparent, lawful protocols. These activities are regulated by the Data Protection Act (2019) in Kenya and the Data Protection Act (2023) in Nigeria. It is recommended that every EdTech startup implement a straightforward, adaptable data management policy that complies with the legal frameworks of its operating region.



3.6 Inclusive Safety and Accessibility

3.6.1 Safety Features

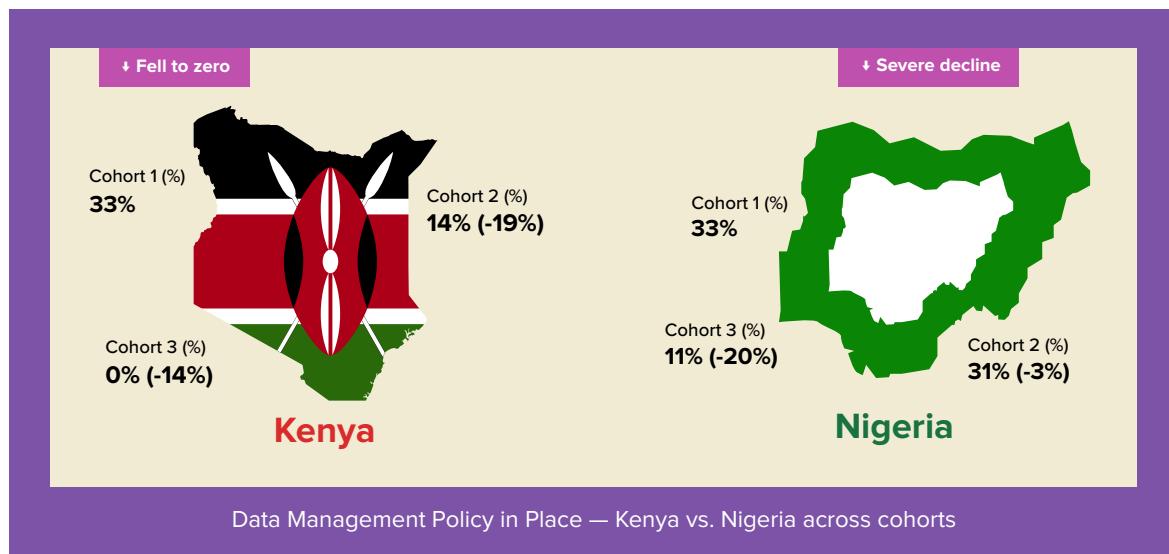
Safety features, including confidential reporting tools, regular audits, and digital safeguards, are essential in protecting learners from harmful content and malicious actors. Their absence directly exposes learners to risk. In Kenya, the implementation of safety features was 71% in cohort 1 and declined continuously (-14%) between Cohorts 1 and 2, and further (-17%) between Cohorts 2 and 3. In Nigeria from 75%, a striking (-35%) decline occurred between Cohorts 1 and 2, with no change between Cohorts 2 and 3. The sustained decline across both countries demands serious attention, particularly given growing global concerns about cybersecurity and AI-related risks in digital learning environments.



3.6.2 Inclusive Reporting

Inclusive reporting entails creating mechanisms that are safe, accessible, and responsive for everyone, regardless of age, gender, ability, literacy level, or social background. Without it, marginalised learners, those often most at risk, are left without a voice. Kenyan startups having a 33% inclusive reporting rate, saw a (-19%) decline between Cohorts 1 and 2, followed by a (-14%) decline in Cohort 3, ending at 0%. Nigeria showed a similar negative trend, a (-3%) decline, also from 33%, between Cohorts 1 and 3, followed by a (-20%) drop between Cohorts 2 and 3, to just 11%. The consistent deterioration in both countries is particularly worrying, as it compounds existing inequalities and effectively silences the most vulnerable users.

Startups should design and test reporting systems with and for diverse users, ensuring accessibility for children, women, learners with disabilities, and marginalised communities. Platforms should also provide multiple reporting channels: text, audio, and visual, to accommodate varied literacy levels.

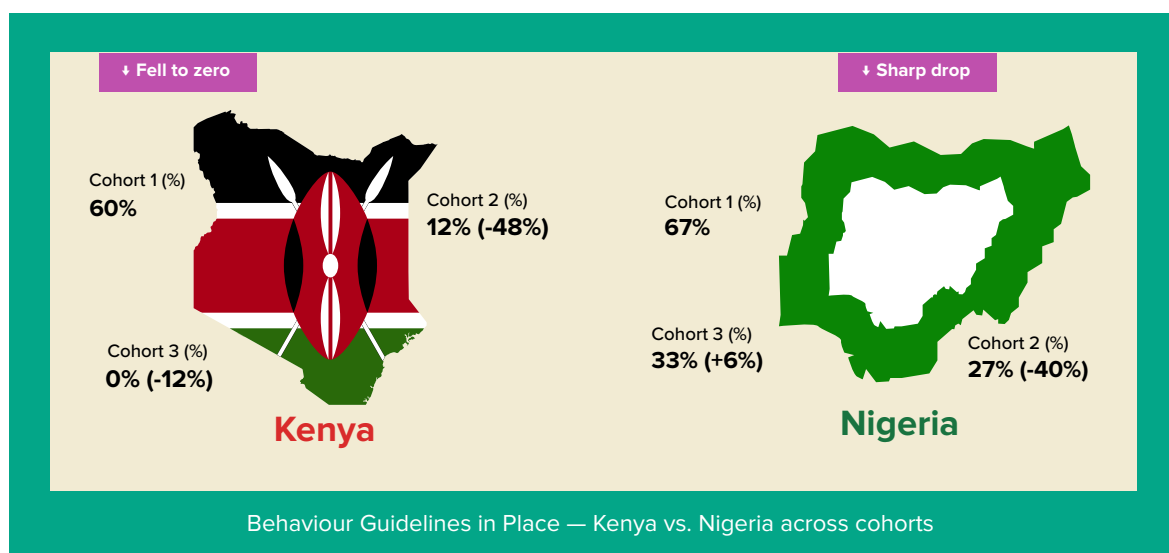


3.7 Content Moderation and Protective Controls

3.7.1 Behaviour Guidelines

Codes of conduct, or behaviour guidelines, establish clear standards for platform interaction and serve as essential instruments for building respectful, safe, and inclusive digital educational spaces. While Kenya initially showed a relatively strong performance with 60% of Cohort 1 startups implementing behaviour guidelines, adoption plummeted by 48% in Cohort 2 and further by 12% in Cohort 3, ultimately reaching 0%, meaning no startup in the third cohort utilised a code of conduct.

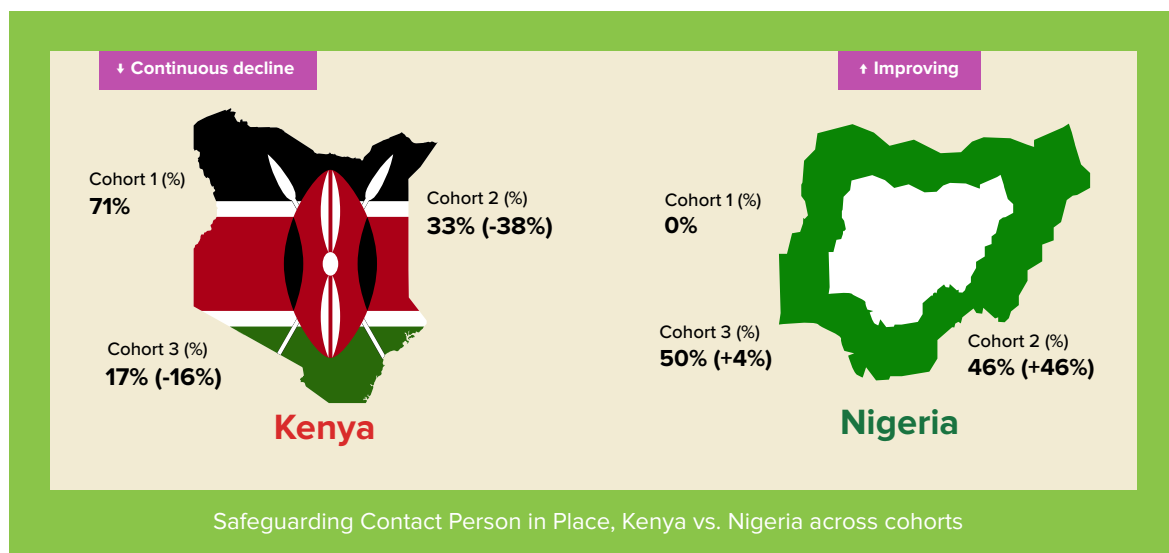
Nigeria followed a similar downward path, starting at 67% in Cohort 1 and dropping by 40% in Cohort 2, before showing a slight 6% recovery to 33% in Cohort 3. The widespread absence of these guidelines across most Edtech platforms thus creates a dangerous void, leaving students susceptible to harassment and misconduct without a structured path for seeking help or resolution. Edtech startups should develop comprehensive Codes of Conduct that define acceptable and prohibited behaviours, outline online communication standards, and establish reporting procedures for misconduct. Such guidelines should be published publicly and integrated into user onboarding.



3.7.2 Safeguarding Contact

Every EdTech startup should have a designated safeguarding officer who serves as the first point of contact, is trained to receive and log reports of suspected abuse, exploitation, or misconduct, and provides confidential guidance to those who raise concerns. Kenya's trajectory is discouraging, 71% in Cohort 1 fell to 33% in Cohort 2, and further to just 17% in Cohort 3. Nigeria shows the opposite trend: starting from 0% in Cohort 1, rising to 46% in Cohort 2 and 50% in Cohort 3. While Nigeria's sustained improvement is encouraging, having a designated safeguarding officer in only half of all startups still falls short of the requirements.

EdTech startups should appoint and publicly identify a Safeguarding Focal Person trained to receive, record, and escalate concerns. Contact details should be visible on every platform page and within all user communications.

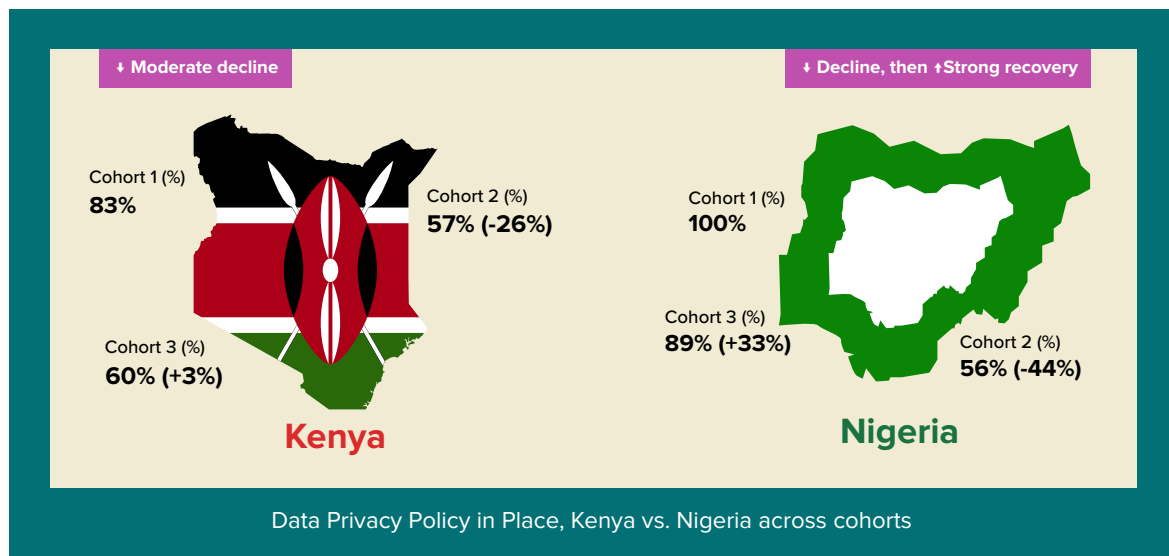


3.7.3 Data Privacy

Data privacy: protecting learners' personal, sensitive, and confidential information is especially critical in safeguarding contexts, where data can relate to abuse, exploitation, or a child's personal circumstances.

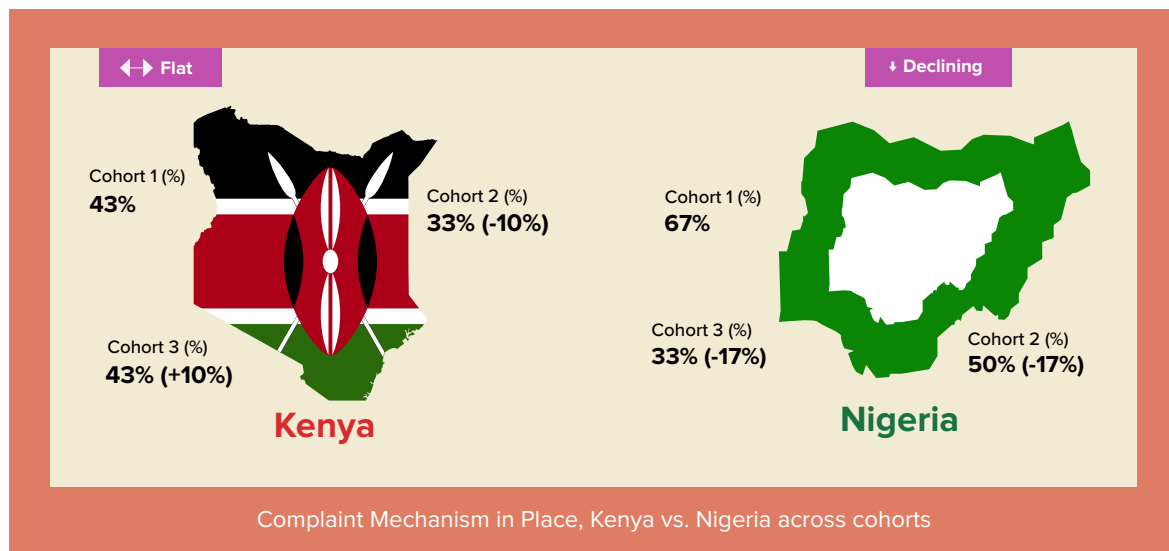
Edtech startups from both countries perform reasonably well. In Kenya, 83% of Cohort 1 startups had a data privacy policy, falling to 57% in Cohort 2 and recovering slightly to 60% in Cohort 3. Nigeria started at 100%, dropped to 56% in Cohort 2, and recovered strongly to 89% in Cohort 3. Nigeria's trajectory here is particularly encouraging, suggesting a growing awareness of data privacy obligations.

There is a critical need for startups to develop integrated safeguarding and privacy policies outlining how child and learner data is collected, stored, shared, and deleted. Such policies should reference the relevant national Data Protection Act and include child-specific consent protocols.



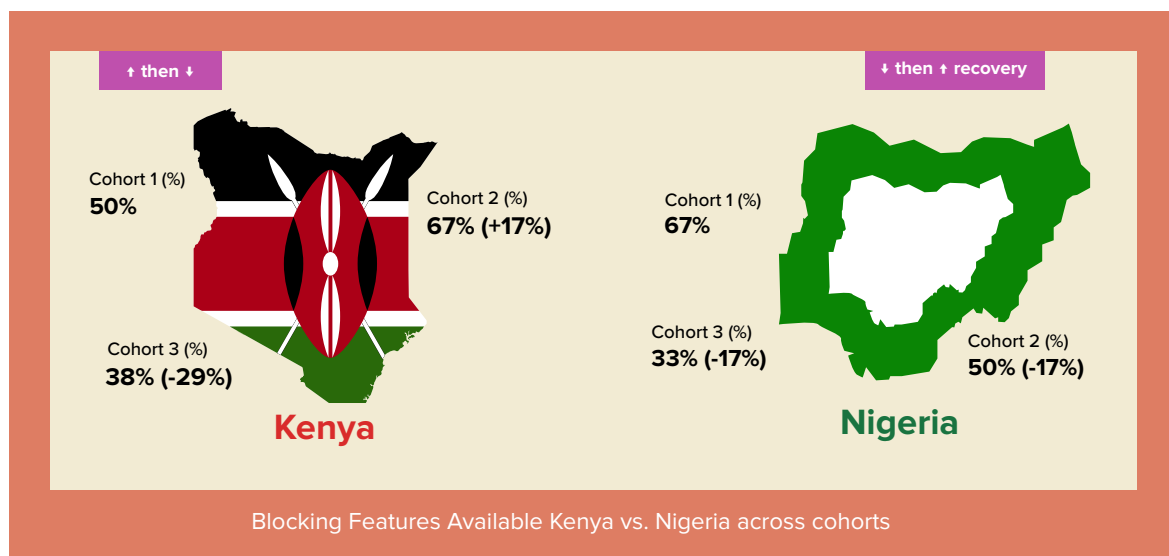
3.7.4 Complaint Mechanism

A complaint mechanism provides users with a trustworthy, accessible, and confidential channel to raise safeguarding concerns. It is distinct from a general reporting mechanism in that it implies a formal process for receiving, investigating, and responding to complaints. Kenya show mixed results, hovering around 43% adoption rate across Cohorts 1 and 3, with a dip to 33% in Cohort 2. Nigerian Edtech startups had a 67% adoption rate in Cohort 1, declined to 50% in Cohort 2, and further to 33% in Cohort 3. The sharp fall in adoption rate in Nigeria, in particular, is a concern for user trust and accountability.



3.7.5 Blocking Features

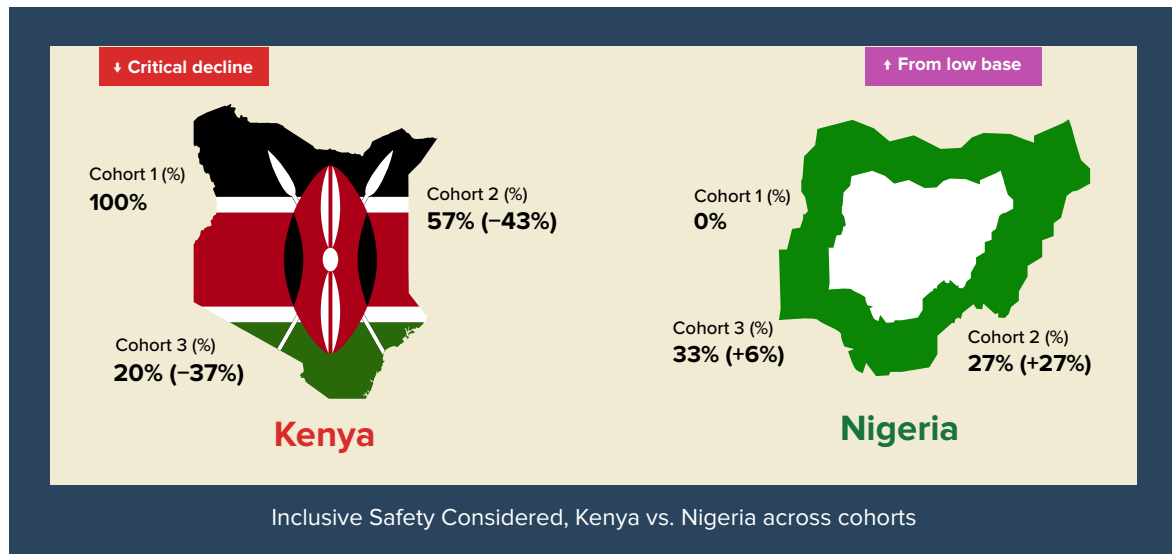
As a core protective measure for learners, blocking features consist of technical controls designed to stop information misuse, restrict access to harmful material, and prevent unauthorised entry. The adoption of these features has seen notable fluctuations. In Kenya, EdTech startups initially reported 50% adoption, which increased to 67% in Cohort 2 before dropping significantly to 38% in Cohort 3. In Nigeria, usage began at 67% but fell sharply to 17% in Cohort 2, with a subsequent partial improvement to 56% in the third cohort. Despite Nigeria's recovery, substantial gaps still persist in both nations, leaving students vulnerable to various digital harms on these platforms.



3.7.6 Inclusive Safety

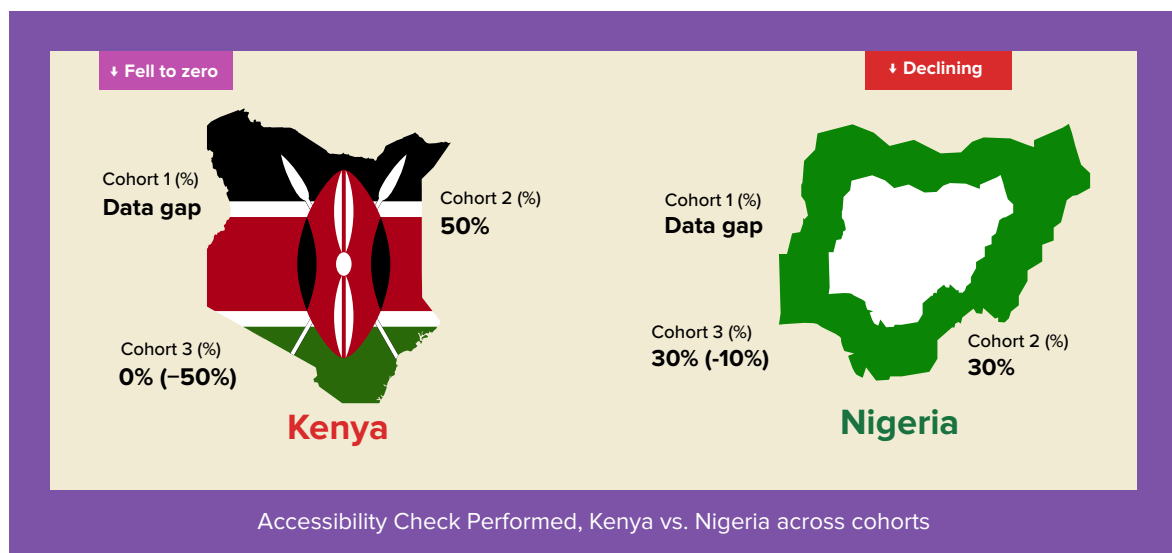
The concept of inclusive safety involves making safeguarding policies, reporting tools, and protective protocols accessible to every child and vulnerable person, moving beyond only those with high digital literacy. In Kenya, this metric started at a full 100% during Cohort 1 but experienced a sharp downturn to 57% in Cohort 2, ultimately falling to a critical 20% by Cohort 3. Conversely, Nigeria began at 0% and has maintained a trajectory of steady growth, reaching 27% in Cohort 2 and 33% in Cohort 3. Despite Nigeria's encouraging progress, it started from a point of total absence, and currently, neither nation has achieved a level of coverage that could be considered sufficient.

Every EdTech startup must develop inclusive policies that explicitly state that safety and safeguarding apply to all users without discrimination.



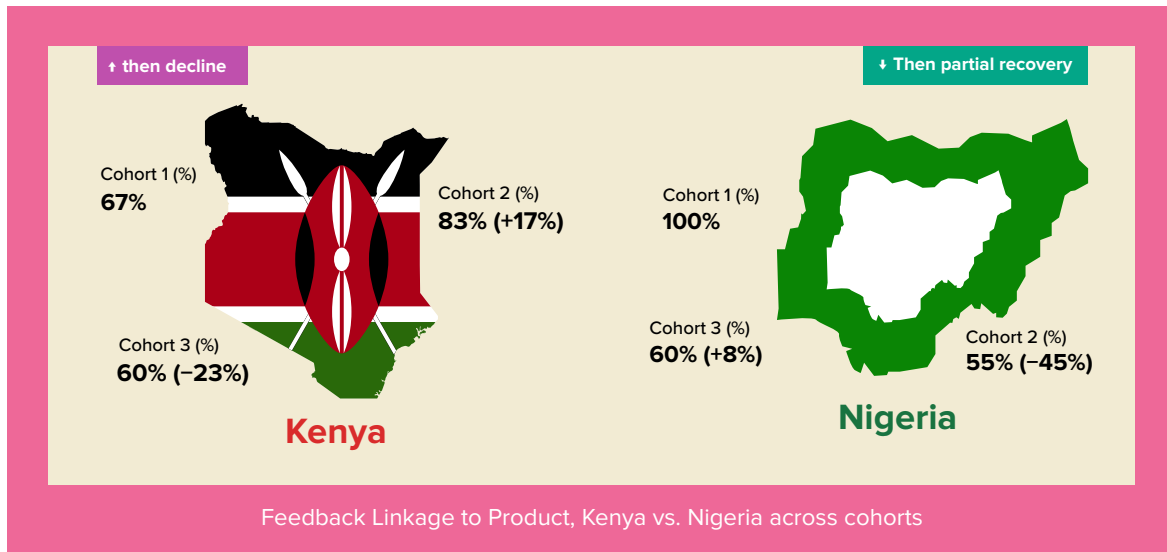
3.7.7 Accessibility Check

Accessibility checks ensure that platform policies, systems, and tools are usable by all learners, including those with disabilities, limited literacy, or low-bandwidth connectivity. Both countries perform poorly in this area. In Kenya, 50% of Cohort 2 startups had conducted accessibility checks, but this fell to 0% in Cohort 3. Nigeria started Cohort 2 at 30% and declined to 20% in Cohort 3. The near-complete collapse of accessibility checking in Kenya, in particular, raises serious concerns about the exclusion of vulnerable learners.



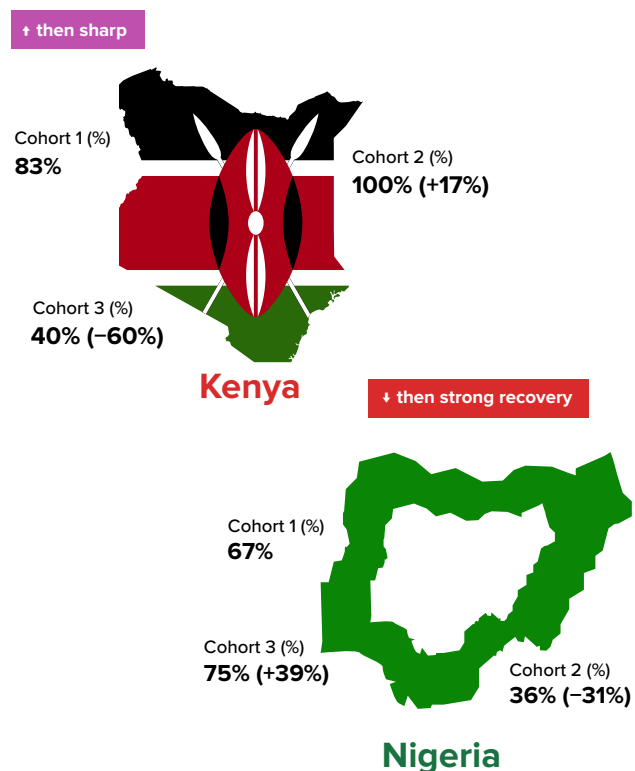
3.7.8 Feedback Linkage

Feedback linkage refers to the collection, analysis, and response to user feedback. When startups listen to and act on what learners tell them, safeguarding systems improve organically over time. This is one of the stronger areas. Kenya started at 67% in Cohort 1, improved to 83% in Cohort 2, and declined to 60% in Cohort 3, which was above average. Nigeria began at an impressive 100% in Cohort 1, dipped to 55% in Cohort 2, and recovered slightly to 60% in Cohort 3, indicating that most startups understood the value of feedback loops, though implementation varied.



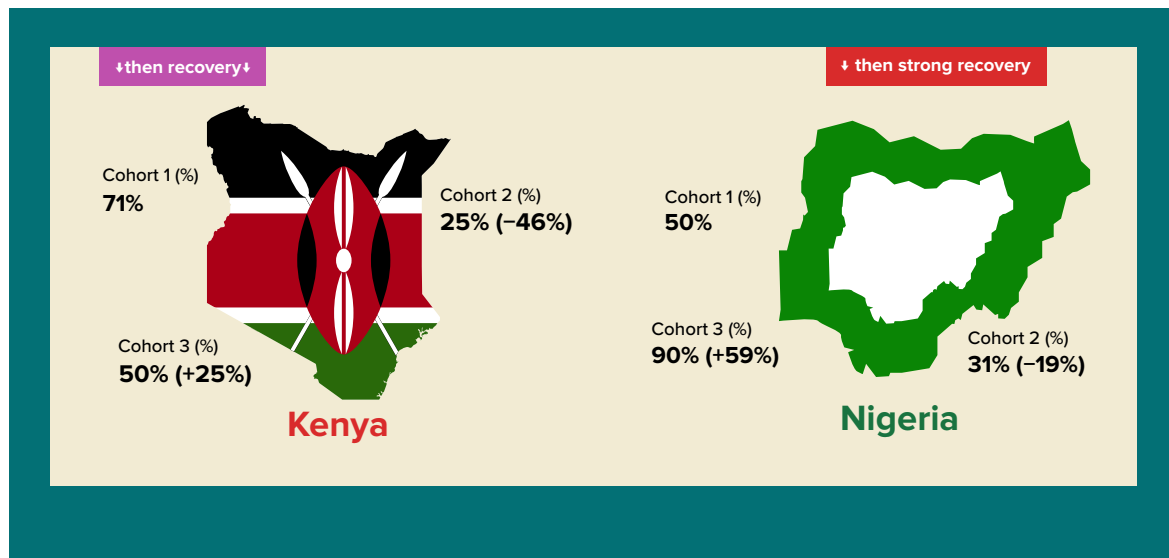
3.7.9 Child-Friendly Terms

Safeguarding, privacy, and usage protocols must be conveyed in language children can actually understand. This is not just good practice; it is a legal and ethical requirement that protects children's rights to informed consent. Kenya performed well overall, with 83% in Cohort 1, reaching 100% in Cohort 2, before a dramatic 60% decline brought the figure to just 40% in Cohort 3. Nigeria started at 67%, experienced a 30.3% decline in Cohort 2, but recovered strongly by (+39%) to reach 75% in Cohort 3. Nigeria's recovery in Cohort 3 is encouraging, while Kenya's sharp decline in the same period is alarming.



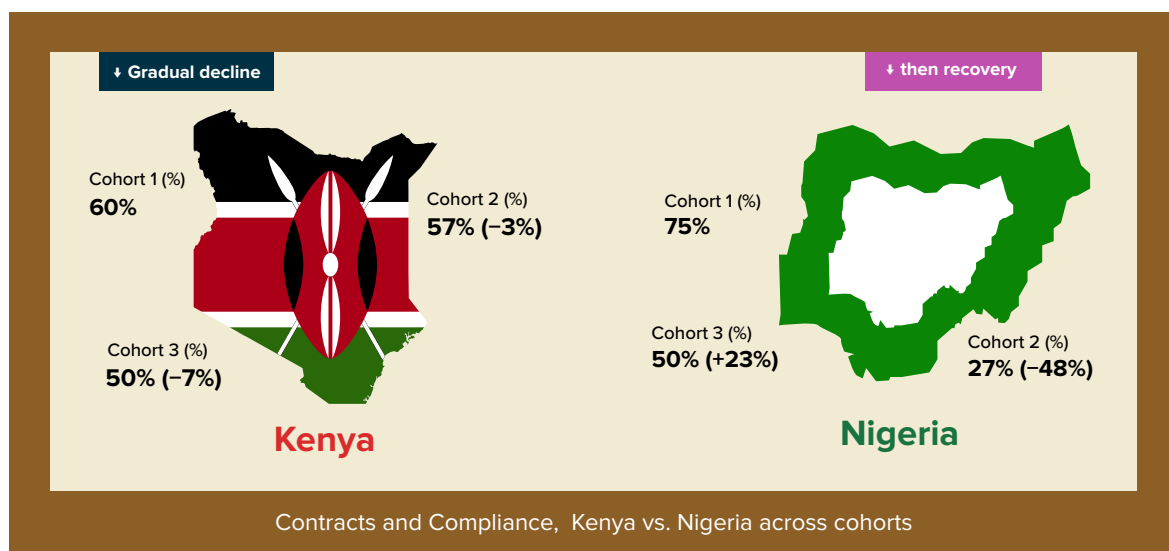
3.7.10 Third Parties

Third-party agreements are formal contracts with external service providers that govern how data, services, and responsibilities are handled. They are critical for legal compliance, data privacy, accountability, and child protection. Kenya had a strong start at 71% in Cohort 1, fell sharply to 25% in Cohort 2, and recovered to 50% in Cohort 3. Nigeria started at 50%, declined to 31% in Cohort 2, and surged to an impressive 90% in Cohort 3. Nigeria's Cohort 3 result suggests growing maturity in third-party governance among its startups.



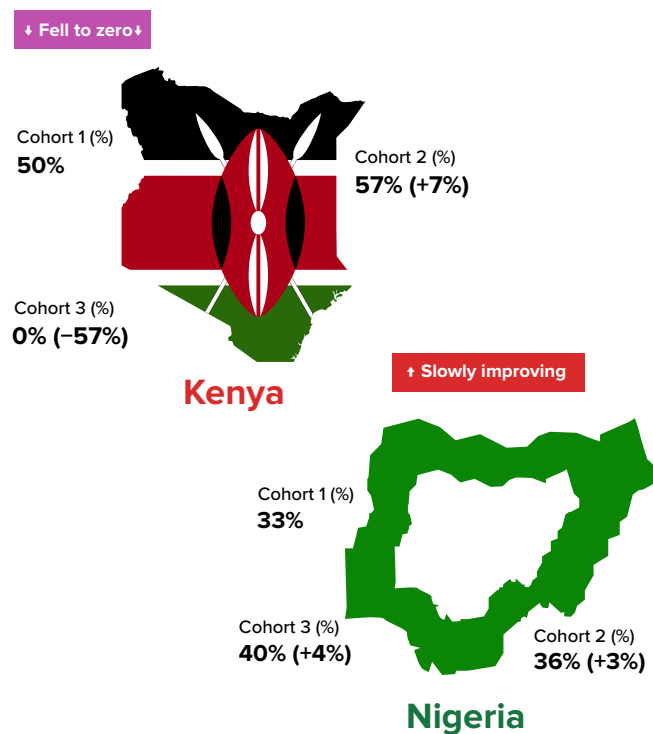
3.7.11 Contracts & Compliance

User agreements, third-party contracts, and employment documents should all include explicit safeguarding clauses and comply with local laws. This provides a legal foundation for safeguarding accountability. Kenya performed above average throughout, starting at 60% in Cohort 1 and declining gradually to 50% in Cohort 3. Nigeria began at 75% in Cohort 1, fell to 27% in Cohort 2, but recovered to 50% in Cohort 3, suggesting awareness of the importance of contracts and compliance, as well as vulnerability to competing pressures that can cause them to slip down the priority list.



3.7.12 Parental Controls

Parental control features allow guardians to monitor and manage a child's digital experience. They are among the most direct ways to extend safeguarding beyond the platform into the home environment. Kenya show a worrying collapse, 50% in Cohort 1, 57% in Cohort 2, then a dip to 0% in Cohort 3. Nigeria maintained a more modest positive trend 33% in Cohort 1, 36% in Cohort 2, and 40% in Cohort 3. However, absolute adoption levels remain way below average. The complete disappearance of parental controls in Kenya's Cohort 3 is concerning, given that over half of Kenyan beneficiaries are children under 18.

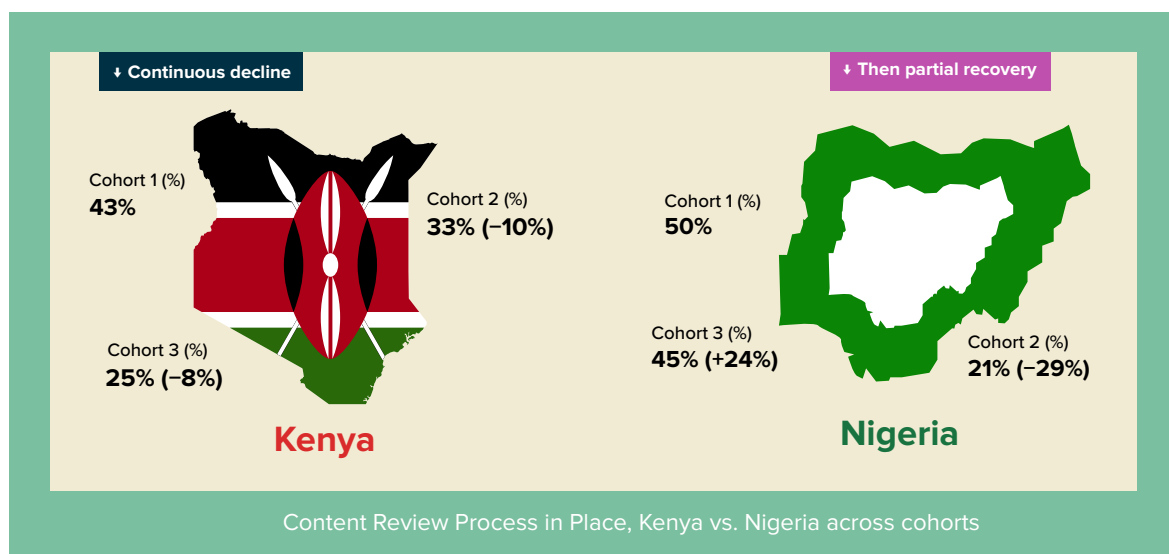


Parental Controls Available, Kenya vs. Nigeria across cohorts

3.7.13 Content Filtering

Content filtering enables users and parents to block harmful or inappropriate material. Without it, children may be exposed to content that no EdTech platform should deliver.

Kenya's adoption has been consistently below average, 43% in Cohort 1, declining to 33% in Cohort 2, and falling further to 25% in Cohort 3. Nigeria started at 50% but dipped to 21% in Cohort 2, recovering partially to 45% in Cohort 3. Content filtering remains one of the most consistently underperforming safeguarding dimensions in both countries.

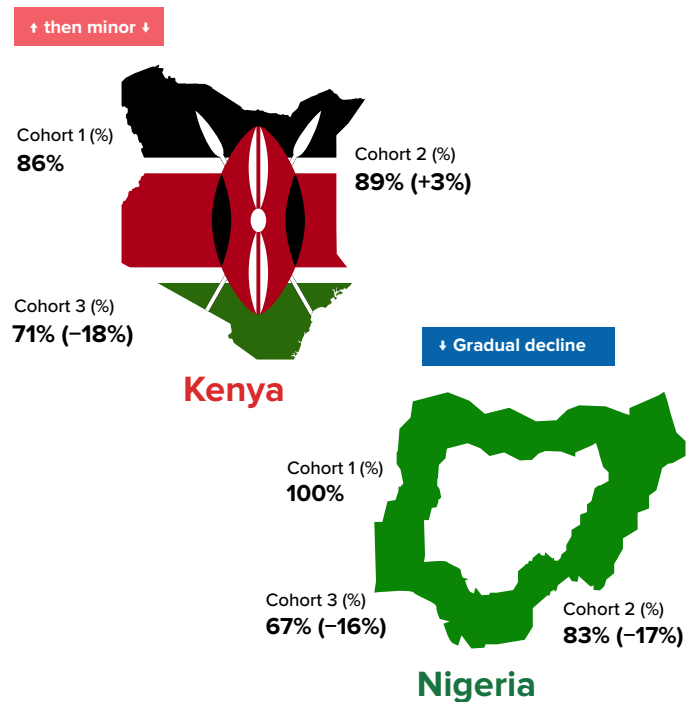


3.8 Product and Platform Safety Reviews

3.8.1 Content Review

Content posted on digital learning platforms must be assessed, moderated, and approved before publication. This is essential to ensure it is safe, inclusive, accurate, and age-appropriate.

This is one of the EdTech programme's strongest areas. Kenya recorded 86% in Cohort 1, rose to 89% in Cohort 2, and dipped only slightly to 71% in Cohort 3. Nigeria achieved 100% in Cohort 1, declined to 83% in Cohort 2, and further to 67% in Cohort 3, still a solid performance. Both countries demonstrate a widespread understanding of the importance of reviewing content before it reaches learners.

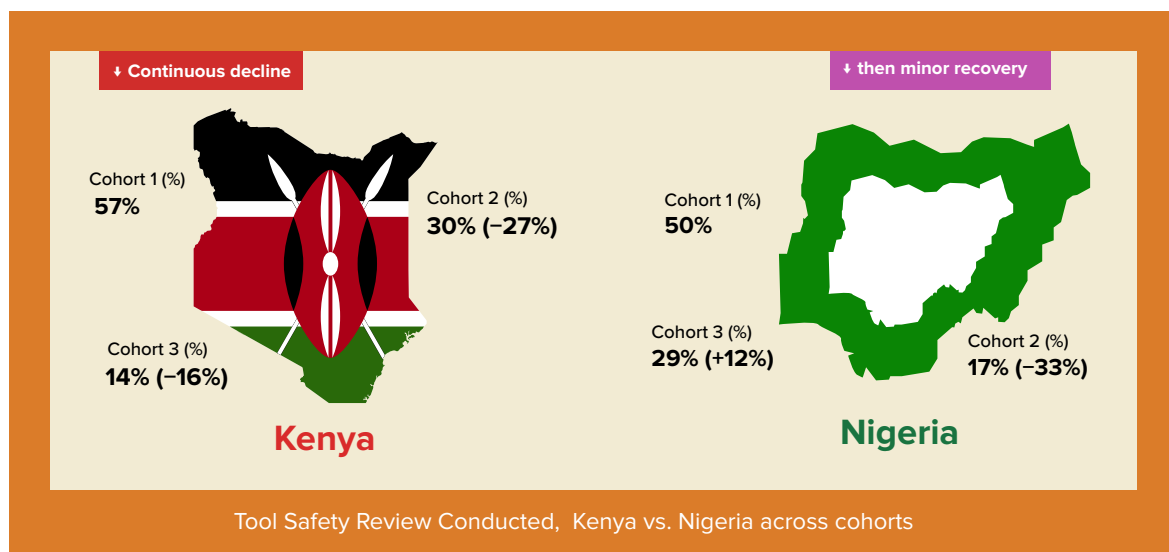


Content Review Process in Place, Kenya vs. Nigeria across cohorts

3.8.2 Tool Safety Review

Tool safety reviews involve assessing the functionality and features of platform tools to ensure they are safe, inclusive, and compliant with safeguarding principles. Without them, potentially harmful tools may reach learners unchecked.

Both countries performed poorly. Kenya began at 57% in Cohort 1, fell to 30% in Cohort 2, and worsened to 14% in Cohort 3. Nigeria started at 50%, declined to 17% in Cohort 2, and recovered marginally to 29% in Cohort 3. Across both countries, the majority of startups are not conducting tool safety reviews before deploying products to learners.

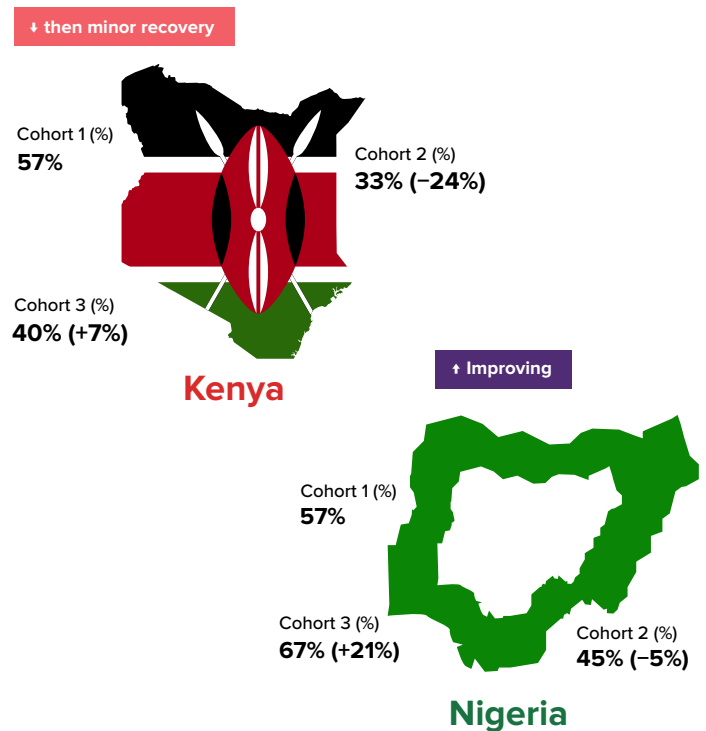


Tool Safety Review Conducted, Kenya vs. Nigeria across cohorts

3.8.3 Platform Safety Review

Platform safety reviews involve a comprehensive evaluation of the entire digital platform to ensure it is safe, inclusive, child-friendly, and compliant with safeguarding principles.

Kenya started at 57%, fell to 33% in Cohort 2, and recovered slightly to 40% in Cohort 3, still below average. Nigeria began at the same 57%, declined slightly in Cohort 2, but rose strongly to 67% in Cohort 3. Nigeria's improvement here is notable, suggesting a growing institutional maturity around platform safety.



Platform Safety Review Conducted, Kenya vs. Nigeria across cohorts

4.0 Emerging Global Safeguarding Trends

This section draws on secondary research covering 603 safeguarding publications curated from Kenya and Nigeria, 53.4% (n=322) from Kenya and 46.6% (n=281) from Nigeria. The analysis provides a broader view of safeguarding priorities, data privacy concerns, and thematic areas that complement and contextualise the primary survey findings.



4.1 Safeguarding Publication Trends

Both Kenya and Nigeria have witnessed a marked surge in publications addressing safeguarding issues between 2001 and 2024. In the early years, activity was minimal. A significant uptick began around 2015, culminating in peak levels in 2023. Kenya experienced a particularly steep rise; publications increased from 1 in 2001 to 72 in 2023. Nigeria's growth was more gradual, reaching 75 publications in 2023. This trend reflects increasing awareness, policy shifts, and the influence of global and continental frameworks on national discourse.

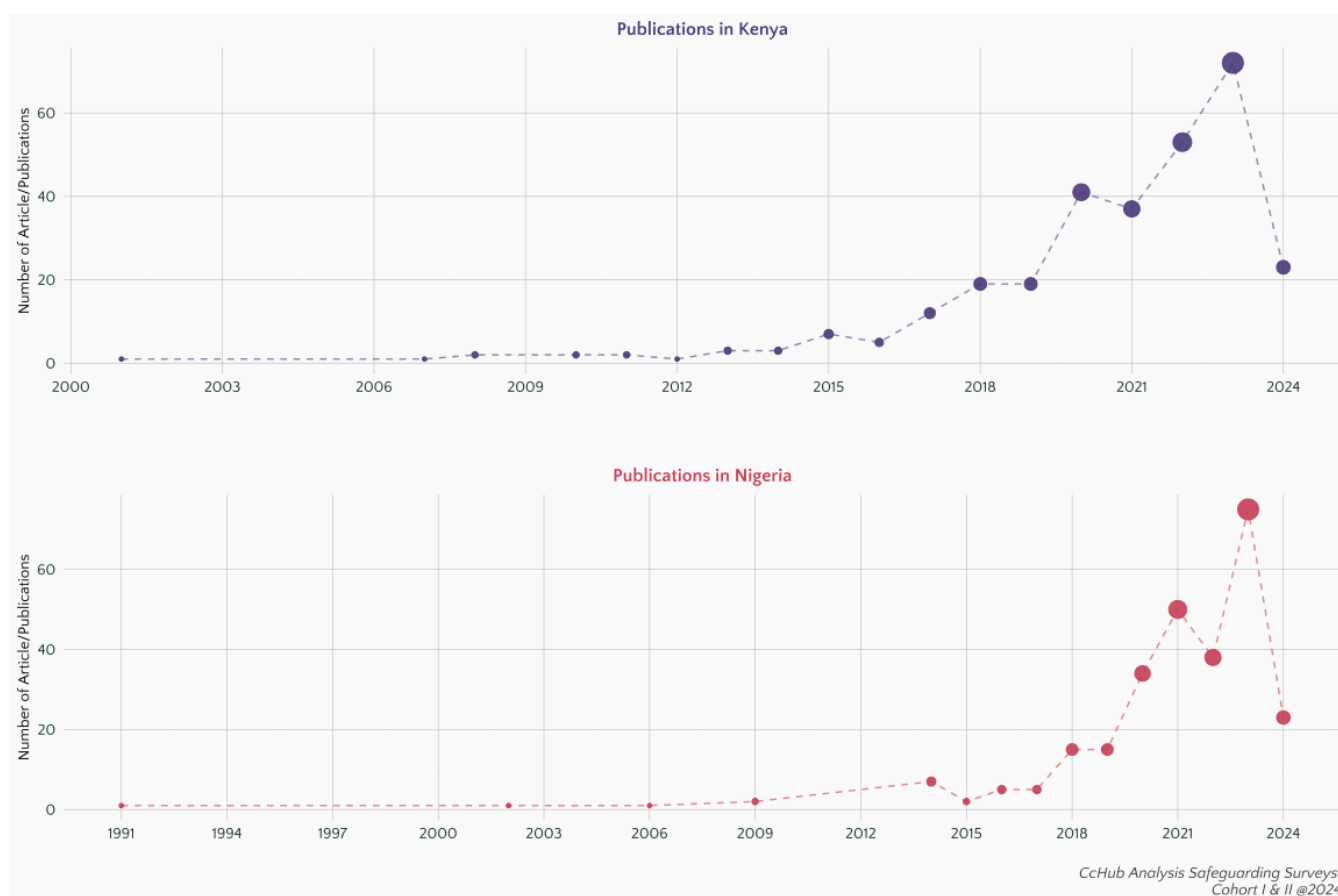


Figure: Safeguarding publication trends in Kenya and Nigeria (1991 to early 2024)

4.2 Data Privacy Concerns

Across all 603 publications, data security and protection emerged as the most universally cited concern. Among the specific issues raised, data sharing and third-party access were most frequently cited (56%), followed closely by data storage and retention (55%), and consent and transparency (50%). Anonymity, confidentiality, data minimisation, and compliance and regulatory issues each featured in around 36% of publications.

Less prevalent but still notable were concerns about unauthorised access, lack of transparency, and access control. Issues such as cybercrime, bias, and surveillance were cited less frequently, suggesting that while awareness exists, these areas may require further attention from researchers and practitioners.

Data Privacy Concern	Frequency (%)
Data Security and Protection	100%
Data Sharing and Third-Party Access	56%
Data Storage and Retention	55%
Consent and Transparency	50%
Anonymity, Confidentiality, and Data Minimisation	36%
Compliance and Regulatory Issues	36%
Unauthorised Access and Lack of Transparency	8-9%
Cybercrime / Bias / Surveillance	<2%

Key data privacy concerns identified across safeguarding publications

4.3 Data Protection and Privacy Systems

Data protection and privacy systems are most widely referenced in the literature. Access controls, data encryption, and data loss prevention were cited in 100% of the reviewed publications, underscoring their status as baseline requirements. Data anonymisation and masking featured in 92% of publications, while compliance frameworks appeared in 68%.

Privacy impact and risk assessments appeared in 55% of publications, and user training in 24%. Notably underrepresented were secure data storage (5%), data governance (4%), data minimisation (11%), and incident response plans (9%). Monitoring and incident response, though critical, were referenced in only 2% of publications.

Data Privacy Concern	Frequency (%)
Access Controls and Authorization	100%
Data Encryption and Security	100%
Data Loss Prevention and Backup	100%
Data Anonymisation and Masking	92%
Compliance and Regulatory Frameworks	68%
Privacy Impact and Risk Assessments	55%
User Training and Awareness	24%
Secure Communication Channels	13%
Data Minimisation	13%
Incident Response Plans	13%
Secure Data Storage	5%
Data Governance	4%
Monitoring and Incident Response	2%

Data protection and privacy systems referenced across publications

4.4 Potential Privacy Risks

Data privacy and security risks were cited in all 603 publications. Compliance and regulatory concerns ranked second at 58%. Technology-related risks appeared in 44% of publications, and inadequate consent mechanisms in 39%. Other critical issues included insufficient data protection practices (23%) and a lack of awareness and training (17%).

Ethical and human rights concerns featured in 17% of articles. Identity theft (4%), digital and social risks (12%), and cultural sensitivity (2%) were cited less frequently but remain important contextual considerations, particularly in the African setting.

4.6 Key Thematic Areas

Analysis of thematic areas across the 603 publications reveals the most prominent concerns in the Kenya and Nigeria EdTech safeguarding landscape. Online safety and cyberbullying emerged as the most frequently emphasised theme overall, featuring in 46% of publications. This was closely followed by data privacy and protection (45%), age-appropriate content (32%), and parental involvement (36%). Emotional and psychological well-being featured in 28% of publications, as did concerns about the digital divide. Misuse of technology was highlighted in 24%, and digital wellbeing in 26%. Policy development stood at 26%, reflecting the recognised need for stronger legislative and institutional frameworks to underpin safeguarding practice in the digital education sector.

4.5 Safeguarding Safety Features

Child protection and data privacy each featured in all 603 publications (100%), underscoring their status as the twin pillars of EdTech safeguarding. Technological and digital safeguarding appeared in 59% of publications, while legal and regulatory compliance featured in 46%. Training, development, and capacity building were highlighted in 37% of documents, reinforcing the primary survey's finding that this area deserves urgent attention.

Risk management and record-keeping were cited in 22% of publications. Multi-agency collaboration and stakeholder engagement featured in 20%, and mental health and wellbeing in 17%. Notably under-represented in the literature are consent mechanisms (3%), physical intervention procedures (2%), and advocacy (1%), areas that may warrant greater scrutiny in future safeguarding research.



Thematic Areas	Kenya (%)	Nigeria(%)	Combined(%)
Emotional and Psychological Well-being	14%	14%	28%
Digital Divide	14%	14%	28%
Digital Wellbeing	13%	13%	26%
Policy Development	13%	13%	26%
Misuse of Technology	12%	12%	24%

5.0 Ecosystem-Level Insights and Implications



The comparative safeguarding analysis across Kenya and Nigeria makes clear that safeguarding challenges are not confined to individual startups; they reflect deeper, systemic gaps within the EdTech ecosystem as a whole. The patterns observed suggest that as accelerator programmes grow, the emphasis placed on safeguarding tends to weaken, leading to declining performance across successive cohorts. This finding demands an ecosystem-level response, not just improvements at the startup level.

5.1 Safeguarding as a Strategic Priority

Although many startups have safeguarding policies in place, implementation remains inconsistent, with up to 100% in some cohorts. Safeguarding is still too often viewed as an administrative formality rather than a core operational and governance priority (Sandvik, 2019). Founders and teams that deprioritise it as they scale are exposing their users to real risks.



Accelerator programmes and investors should integrate safeguarding performance metrics into funding and reporting requirements. Founders should be required to present safeguarding updates during programme review sessions.

5.2 Safeguarding Fatigue Across Cohorts

The analysis consistently reveals declining trends in risk assessments, risk registers, and inclusive design indicators across later programme cohorts (Inclusive Futures, 2025). Inclusive safety in Kenya fell from 100% to 20%, and accessibility checks dropped to 0%. These are not marginal declines; they represent a near-total collapse of important safeguarding practices in some dimensions.



Introduce a safeguarding performance tracker across accelerator cohorts to monitor consistency. Funding release should depend on meeting minimum safeguarding criteria, not only business performance milestones.

5.3 Weak Training Culture

Safeguarding training rates for staff and associates declined in both Kenya and Nigeria, suggesting that many teams are operating without adequate awareness of safeguarding principles and response procedures. Without trained staff, even excellent policies cannot be effectively implemented.



Make safeguarding training mandatory and regular for all startup teams, mentors, and contractors during induction. Include refresher sessions in every accelerator cycle.

5.4 Inclusion and Accessibility Gaps

The deterioration in inclusive reporting and accessibility checks is particularly troubling. It points to the progressive exclusion of vulnerable groups, learners with disabilities, those with limited literacy, and those from marginalised communities, from the very safeguarding systems that are supposed to protect them most (Able Child Africa & Save the Children International, 2021).



Develop clear accessibility standards for EdTech solutions. Platforms should offer multiple reporting channels: audio, visual, and text, and provide low-literacy options throughout.

5.5 Data Management as a Strength to Build On

Data privacy and management remain one of the strongest safeguarding areas across both countries, with up to 100% compliance in Nigeria's later cohorts. This represents a genuine foundation that can be extended.



Build on this momentum by integrating child-specific privacy protocols, including informed consent for learners, limited data profiling, and anonymisation for sensitive datasets.

5.6 Governance and Accountability Weaknesses

Few startups have designated safeguarding focal persons, reducing individual accountability. Without a clear governance structure, even robust policies tend to fail at implementation, as there is no single person responsible for ensuring they are followed.



Require all startups to appoint trained safeguarding officers, with their contact details prominently displayed on their platforms. Accelerators should establish shared monitoring and escalation systems.

5.7 Fragmented Safety Reviews

While content review remains relatively strong, tool and platform safety checks are inconsistent. Many products are being deployed to learners without adequate pre-launch safety testing, a situation that is difficult to justify when the majority of beneficiaries are children.



Implement structured product safety reviews and pre-deployment audits as a standard component of accelerator quality assurance.

5.8 Towards a Collaborative Ecosystem

The trends across cohorts demonstrate that safeguarding cannot be improved by individual startups acting alone. The evidence calls for a coordinated effort involving accelerators, regulators, education ministries, and funders.



Establish a Regional EdTech Safeguarding Forum involving accelerator programmes, regulators, and education ministries. The Forum would harmonise safeguarding policies, share training resources, and monitor progress annually.

6.0 Conclusion



The incorporation of digital technology into education, particularly across Africa following the COVID-19 pandemic, represents a transformative shift towards improved access to quality learning. However, the rapid adoption of EdTech solutions in Kenya, Nigeria, and other African countries poses important safeguarding challenges that demand serious and sustained attention.

The analysis of safeguarding self-audit data from the EdTech programme, combined with secondary research, reveals significant gaps in current safeguarding practice among educational startups in both countries. Safeguarding policies often lack the specificity needed to address the unique challenges of digital platforms. Training is inconsistent or absent. Risk registers are effectively nonexistent in some start-ups. Inclusive design features are deteriorating. Moreover, the critical role of a designated safeguarding officer is neglected, particularly among Kenyan startups.

At the same time, the data tells a more nuanced story. Content review, data management,

and feedback linkage remain areas of relative strength. Nigeria demonstrates promising improvements in platform safety review and third-party agreements. These positive signals are worth celebrating and should serve as the foundation for extending the safeguarding culture more broadly.

The right to privacy is increasingly protected by national legislation in both countries, and by international frameworks such as GDPR and COPPA. Yet, data protection and privacy considerations in some EdTech products do not always align with these frameworks and often fail to adequately protect children and vulnerable adults. Stakeholders across the ecosystem, including the programmes themselves, EdTech startups, users, policymakers, and other educational actors, must prioritise child data protection and wellbeing as non-negotiable features of responsible EdTech development. Ultimately, safeguarding must evolve beyond startup-level actions to become a coordinated ecosystem strategy. Timely, intentional, and effective adoption of safeguarding practices ensures that EdTech solutions serve as tools

for equitable and secure education rather than become sources of risk for the children and young people they are meant to serve.

7.0 Recommendations

The analysis demonstrates an urgent need for a coordinated, sector-wide approach to safeguarding across EdTech startups, accelerators, and investors. The following recommendations are drawn from both the survey findings and the secondary landscape research. They are structured around the key gaps identified throughout this report.



7.1 For EdTech Startups

Comprehensive Safeguarding Policies

Design and implement robust safeguarding policies tailored to EdTech digital environments. Policies should include clear protocols for data handling, user consent, children's rights in digital spaces, and incident response procedures. Policies must be reviewed by internal experts and updated regularly.

Safety-by-Design from Day One

Integrate safety-by-design practices into every stage of product development and deployment. Anticipate and mitigate safeguarding risks related to content, conduct, and contact before releasing products to learners.

Mandatory Staff Training

Ensure that all staff, mentors, and contractors complete certified safeguarding training modules before platform deployment. Refresher training should be conducted at least annually and whenever new products or features are launched.

Maintain an updated Safeguarding Risk Register	Establish and regularly update a formal safeguarding risk register documenting identified risks, their likelihood, potential impact, and SMART mitigation strategies. This should be a living document, not a one-time exercise.
Appoint a Safeguarding Focal Person	Designate a trained safeguarding officer whose contact details are visible on every platform page and in all user communications channels. This person should be empowered to receive, record, and escalate concerns.
Inclusive and Child-Friendly Design	Ensure that reporting mechanisms, privacy terms, and usage guidelines are accessible to all learners, including those with disabilities, limited literacy, or low bandwidth. Offer multiple reporting channels (text, audio, visual) and translate safeguarding content into a language children can understand.
Transparent Data Practices	Adopt integrated safeguarding and privacy policies that reference the relevant national Data Protection Act. Publicly share data protection measures, complaint procedures, and incident reporting mechanisms to build trust with users and guardians.

7.2 For Accelerators and Funders

- Integrate safeguarding performance metrics into funding and reporting requirements. Tie funding milestones directly to safeguarding outcomes, not only commercial performance.
- Integrate safeguarding performance metrics into funding and reporting requirements. Tie funding milestones directly to safeguarding outcomes, not only commercial performance.
- Integrate safeguarding performance metrics into funding and reporting requirements. Tie funding milestones directly to safeguarding outcomes, not only commercial performance.
- Integrate safeguarding performance metrics into funding and reporting requirements. Tie funding milestones directly to safeguarding outcomes, not only commercial performance.
- Integrate safeguarding performance metrics into funding and reporting requirements. Tie funding milestones directly to safeguarding outcomes, not only commercial performance.



7.3 For the Broader Ecosystem

- Establish a Regional EdTech Safeguarding Forum involving accelerator programmes, regulators, and education ministries to harmonise policies, share resources, and monitor annual progress.
- Create shared safeguarding scorecards and publish annual progress summaries across the sector.
- Embed safeguarding metrics into all EdTech funding and accelerator assessment frameworks at the ecosystem level.
- Conduct follow-up studies to track whether interventions improve safeguarding over time, creating an evidence base for continuous improvement.
- Engage continuously with regulatory bodies to ensure EdTech practices align with evolving legal and legislative frameworks protecting children's rights.



8.0 References

- Day, E., Pothong, K., Atabey, A., & Livingstone, S. (2022). Who controls children's education data? A socio-legal analysis of the UK governance regimes for schools and EdTech. *Learning, Media and Technology*, 49(3), 356–370.
- Johnson, A. K., & Sloth-Nielsen, J. (2020). Child protection, safeguarding and the role of the African Charter on the Rights and Welfare of the Child: Looking back and looking ahead. *African Human Rights Law Journal*, 20(2), 643–666.
- Nassimbwa, J., Kakuru, M. D., & Mpamizo, T. M. (2022). Locating State Actors in Violence against Children (VAC) Networks in Kenya: A Complexity Leadership Lens. *International Journal of Child, Youth and Family Studies*, 13(2-3), 123–142.
- Olusegun, O. O., & Olarinde, S. (2017). Child Rights Protection in Nigeria and the United Kingdom: Lessons for Nigeria. *African Journal of Law and Human Rights*, Vol. 1.
- Onyemachi, T. (2010). Children, Status and the Law in Nigeria. *African Research Review*, 4(3).
- UNHCR. (2002). Sexual Violence and Exploitation: The Experience of Refugee Children in Liberia, Guinea, and Sierra Leone.

- Walker, K. L., Bodendorf, K., Kiesler, T., de Mattos, G., Rostom, M., & Elkordy, A. (2023). Compulsory technology adoption and adaptation in education: A looming student privacy problem. *Journal of Consumer Affairs*, 57(1), 445–478.
- Sandvik, K. B. (2019). 'Safeguarding' as a humanitarian buzzword: An initial scoping. *Journal of International Humanitarian Action*, 4(1), Article 2. <https://link.springer.com/article/10.1186/s41018-019-0051-1>
- Inclusive Futures. (2025, August). Practical pathways for disability inclusive safeguarding: How development and humanitarian programmes can deliver inclusive safeguarding that protects children and adults with disabilities. https://inclusivefutures.org/wp-content/uploads/2025/08/Inclusive-Futures_safeguarding-report_accessible.pdf
- Able Child Africa, & Save the Children International. (2021). Disability-inclusive child safeguarding guidelines https://ablechildafrica.org/wp-content/uploads/2021/05/Able_Child_Africa_Save_The_Children_DiCS_Guidelines_Full.pdf
- Chambers, D., Cantrell, A., & Booth, A. (2021). Recognition of risk and prevention in safeguarding of children and young people: a mapping review and component analysis of service development interventions aimed at health and social care professionals. *BMC Health Serv Res*. doi: 10.1186/s12913-021-07257-8
- UNICEF. (2026). Child Safeguarding Toolkit for Business: 2026 Edition. <https://www.unicef.org/childrightsandbusiness/media/1681/file/Child-Safeguarding-Toolkit-2026.pdf>
- Grant, B. (2026). Framing child protection systems: Toward a normative framework and operational definition for policy and practice, *Child Protection and Practice*. Volume 8. <https://doi.org/10.1016/j.chipro.2026.100277>.