Digital Initiative For Innovation & Development



Child Online Safety Legislation Across Africa

A Policy Analysis

July, 2026

Table of Contents

Executive Summary	**1**
1. Introduction	**2**
2. The State of Play	**3**
2.1. The Numbers	3
2.2. The Patterns	5
3. Structural Gaps	**7**
Gap 1: The Platform Accountability Deficit	7
Gap 2: Age Verification and Child-Specific Data Protection	7
Gap 3: The Enforcement and Institutional Capacity Deficit	7
Gap 4: The Participation and Evidence Deficit	8
Gap 5: Digital Literacy and Prevention	8
4. Drivers and Barriers to Implementation Progress	**9**
4.1. Drivers	9
4.2. Barriers	9
5. Advocacy Recommendations	**10**
5.1. Civil Society Organisations	**10**
1. Prioritise domestication of the AU COP Policy	10
2. Build a national COP coalition modelled on Nigeria's approach	10
3. Use DPAs as strategic entry points	10
4. Insist on rights-respecting design	10
5.2. For the African Union and Regional Economic Communities	**12**
1. Develop an AU COP Policy implementation scorecard	12
2. Leverage RECs for sub-regional harmonisation	12
5.3. For International Development Partners and Donors	**12**
1. Fund implementation, not just legislation	12
2. Commission Africa-specific evidence	12
3. Support platform accountability mechanisms	12
5.4. For Technology Platforms	**12**
1. Apply global standards uniformly	12
2. Invest in African-language content moderation	13
Strategic Priorities: Where to Focus First	**13**
6. Conclusion	**14**

Executive Summary

Africa's over 500 million children are going online faster than the laws designed to protect them are being written. Only five of the continent's 55 countries have enacted dedicated, enforceable child online safety legislation with legal force, while the majority rely on general cybercrime provisions or penal codes with tangential relevance. A handful have no relevant legal framework at all.

The last 3 years, 2023–2025, were a breakthrough period for the continent. The African Union (AU) adopted the world's first regional Child Online Safety and Empowerment Policy. In the same period, countries like Tanzania, Cameroon, Kenya, and Kenya all advanced significant legislative or regulatory instruments, proposed related draft bills, or issued their first children's data directives.

However, a wide gap remains in the legal frameworks of African countries for addressing various issues related to child online protection. Even countries with advanced regulatory frameworks, such as South Africa and Nigeria, lack dedicated, standalone Child Online Protection (COP) legislation. It is also interesting to note that while about 46 countries have specific legislation covering cybercrimes, this high uptake/political will is not reflected in the number of protection- or rights-based frameworks, especially for children.

1. Introduction

In February 2024, the African Union (AU) adopted the Child Online Safety and Empowerment Policy[1], which established a framework for member states to ensure that children (anyone under the age of 18) are protected, empowered, and able to thrive in the digital environment. This policy piggybacks on the African Charter on the Rights and Welfare of the Child and the African Union Convention on Cybersecurity and Personal Data.

This policy is becoming increasingly significant given Africa's youthful demographic profile. Children account for approximately 47% of the continent's population, representing nearly half of all Africans[2]. As internet access, smartphone ownership, and digital participation continue to expand across the continent, millions of children are increasingly exposed to both the opportunities and risks of the online environment.

While digital technologies can enhance learning, creativity, and civic participation, they can also expose children to cyberbullying, online exploitation, harmful content, privacy violations and other forms of digital harm.

Since the adoption of the policy, AU member states have progressed at varying speeds in aligning their national frameworks with the Child Online Safety and Empowerment Policy. While some countries have enacted dedicated child online protection laws, regulations, or implementation guidelines, others continue to rely on broader cybersecurity, child protection, or data protection legislation that only partially addresses the online risks children face. As a result, the landscape of child online safety in Africa remains uneven.

This policy brief maps out the level of enactment across the continent. It also identifies five structural gaps in the current landscape, analyses the political and institutional dynamics shaping policy movement, and sets out targeted advocacy recommendations for civil society, regional bodies, and development partners.

1 African Union. (2024, February). The African Union child online safety and empowerment policy. African Union Commission.

2 UNICEF. (n.d.). How many children are there in Africa? UNICEF Data. Retrieved June 6, 2026, from UNICEF Data – How many children are there in Africa?

2. The State of Play

A comprehensive mapping of 54 AU member states (see companion document) reveals a highly uneven and rapidly shifting continent, marked by a persistent gap between formal legal adoption and meaningful enforcement.

2.1. The Numbers

There are 5 countries in Africa that have enacted dedicated enforceable child online safety laws/regulations with legal backing: **Ghana** (Cybersecurity Act 2020 with child-specific provisions; COP Framework 2024)[3], **Mauritius** (ICTA COP Directive implementing binding COP standards)[4], and **Tanzania** (Child Protection Laws Miscellaneous Amendments Act 2024, amending the Cybercrimes Act)[5]. **Kenya** (CA's Industry Guidelines for COP, effective October 2025, binding on licensed ICT providers)[6] and **Cameroon** (Charter on Child Online Protection in Cameroon - Law No. 2023/009 of July 25, 2023)[7] have robust, multi-layered COP systems, but no standalone COP law.

Only 3 countries have dedicated COP bills or policies in draft: **Nigeria** (Child Online Access Protection Bill HB.244 passed House Dec 2025, awaiting Senate)[8]; **Rwanda** (Ministerial Order on COP Jan 2024 and 5-Year Action Plan, but primary COP legislation reportedly under

3 Cyber Security Authority. (2024). National child online protection framework. Government of Ghana. https://www.csa.gov.gh/resources/National%20COP%20Framework.pdf

4 Information and Communication Technologies Authority. (2025, December 1). Telecommunication Directive 4 of 2025 (TD 4 of 2025): Child online protection measures. Government of Mauritius.

5 Office of the Attorney General. (n.d.). OAG-MIS: Online laws catalogue. United Republic of Tanzania. Retrieved June 6, 2026, from https://oagmis.oag.go.tz/

6 Communications Authority of Kenya. (2025, April). Industry guidelines for child online protection and safety in Kenya. Communications Authority of Kenya. https://www.ca.go.ke/sites/default/files/2025-04/%20Industry%20Guidelines%20for%20Child%20Online%20Protection%20%28COP%29%20and%20Safety%20in%20Kenya_Apr2025.pdf

7 Ministère des Postes et Télécommunications Accessible Law. (4 July 2023) Charter on Child Online Protection in Cameroon: Adopted by Parliament https://www.minpostel.gov.cm/index.php/en/actualites/458-charter-on-child-online-protection-in-cameroon-adopted-by-parliament

8 Emejo, J. (2026, May 27). Experts urge Senate to speed up passage of child online safety bill amid rising digital threats. ThisDay. ThisDay article

consideration and not yet enacted; Budapest Convention accession Jan 2025)[9] and **Zimbabwe** also has a draft Child Online Protection Policy under development.[10]

Also, 3 countries have launched dedicated national COP strategies without tangible legislative backing: Zambia (National COP Strategy 2025–2029, launched Nov 2025)[11], Malawi (draft National COP Strategy; MACRA COP Initiative launched Feb 2025)[12], and Lesotho (COP Guidelines 2024, transposing ITU Guidelines)[13].

Over 30 countries rely on general cybercrime legislation, penal codes, or data protection laws that contain provisions tangentially relevant to child online safety, criminalising child pornography or providing general data protection, but lack dedicated COP frameworks. This is the largest category and includes significant digital economies, such as Egypt, Algeria, Ethiopia, Morocco, Côte d'Ivoire, Uganda, and Senegal.

Only 5 countries have no identifiable legislation, regulations, or policy frameworks addressing child online safety in any form: Eritrea, Libya, Gambia, Guinea-Bissau, and Burundi.

9 Council of Europe. (2025, January 15). Rwanda becomes the 78th Party to the Convention on Cybercrime and accedes to the First Protocol. Cybercrime Programme Office, Council of Europe. https://www.coe.int/en/web/cybercrime/-/rwanda-becomes-the-78th-party-to-the-convention-on-cybercrime-and-accedes-to-the-first-protocol

10 Makaripe, T. (2026, June 3). Zimbabwe approves policy to protect children from online abuse. Children's Voice. https://childrensvoice.co.zw/2026/06/03/zimbabwe-child-online-abuse-policy/

11 UNICEF Zambia. (2024, October 11). *Children request investments in digital literacy and child-friendly reporting mechanisms*. UNICEF. https://www.unicef.org/zambia/press-releases/children-request-investments-digital-literacy-and-child-friendly-reporting

12 Paradigm Initiative. (2024, June). Malawi country report (Londa Digital Rights and Inclusion in Africa Report 2023/2024). Paradigm Initiative. https://paradigmhq.org/wp-content/uploads/2024/06/Malawi-Country-Report.pdf

13 International Telecommunication Union. (2020). Child online protection guidelines. International Telecommunication Union. https://www.itu-cop-guidelines.com/

Classification Note

The distinction between "Enacted" and "Partial/Advanced Framework" matters for advocacy. Countries like South Africa and Kenya have robust, multi-layered protection systems that, in many respects, are more effective than some standalone COP laws. But the absence of a dedicated COP statute creates legal fragmentation, potential coverage gaps, and vulnerability to piecemeal amendments or the weakening of individual instruments. Advocacy for standalone legislation in these countries should not be read as criticism of existing frameworks but as a case for consolidation and strengthening.

2.2. The Patterns

The period 2023–2025 saw **more dedicated COP legislative and regulatory action than all previous years combined**. Tanzania's 2024 amendments, Kenya's binding COP Guidelines, and Nigeria's HB.244 all followed in rapid succession. This reflects the catalytic effect of the AU COP Policy (February 2024) and intensified UNICEF/ITU engagement across the continent.

Francophone Africa is also showing political/legislative motivation on the topic. Cameroon introduced its Draft Law No. 2023/009, with the members of the lower house adopting it. Senegal and Mali's DPAs issued children's data directives in 2024. Djibouti adopted a Digital Code in 2025. Gabon introduced a Social Media Age Verification Ordinance in 2026. The Francophone lag is narrowing, driven in part by engagement from the ECOWAS Commission and the Council of Europe.

COP guidelines and strategies are also increasing in number, but are not core legislation. Zambia's National COP Strategy (2025–2029), Malawi's draft COP Strategy, Lesotho's COP Guidelines (2024) and Eswatini's five-part COP Guidelines represent a significant expansion of the policy landscape. However, guidelines and strategies, even if binding on regulated entities (as Kenya's), lack the permanence, comprehensive scope, and enforcement teeth of primary legislation. This distinction matters for long-term protection.

Data protection authorities remain strategic entry points. The 2024 directives from Mali and Senegal's DPAs, Kenya's ODPC enforcement actions regarding children's photos, and South Africa's Information Regulator's participation in international age-assurance initiatives confirm that DPAs are emerging as important institutional actors for child online safety, even where dedicated COP legislation does not exist.

Continental policy without national domestication remains the core risk. While the AU COP Policy (February 2024) is the first regional COP policy globally, the Malabo Convention's[14] 9-year wait to reach the 15 ratifications required for entry into force, and the fact that major digital economies remain absent, serve as cautionary precedents. Without active domestication pressure, the COP Policy risks the same trajectory.

14 African Union. (2014, June 27). African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). African Union. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

3. Structural Gaps

Gap 1: The Platform Accountability Deficit

Across most of the continent, global technology platforms operate without binding child safety obligations. Even among the five countries with enacted COP instruments, platform accountability provisions vary dramatically. The platforms that pose the greatest risk: social media, messaging apps, gaming, and AI-powered services, are headquartered outside the continent and operate under frameworks designed in different jurisdictions.

Gap 2: Age Verification and Child-Specific Data Protection

Age verification is foundational, as you cannot protect children online without identifying them. Yet robust age verification requirements exist in only a handful of jurisdictions. Kenya's Guidelines require "age verification mechanisms," but technical standards for compliance are not yet specified. Gabon's 2026 Social Media Age Verification Ordinance[15] is a notable development in Francophone Africa. South Africa's POPIA requires consent from competent persons for the collection of children's data. Rwanda's 2024 ministerial order requires parental consent for publishing children's images. But most of Africa's over 36 data protection laws define an age of consent for data processing without addressing design obligations, transparency requirements, or profiling restrictions specific to children.

Gap 3: The Enforcement and Institutional Capacity Deficit

The most advanced legislation is only as effective as the institutions tasked with enforcing it. Across most of the continent:

- Digital forensic capabilities are concentrated in a small number of countries. Most law enforcement agencies lack the technical capacity to investigate online child exploitation.
- Cross-border cooperation mechanisms remain underdeveloped.
- Even well-designed legislation faces rights risks in implementation. South Sudan's Cybercrimes Act 2026 has drawn criticism from CPJ and human rights organisations for its vague definitions of "false information" and "undesirable content," which could suppress press freedom and civil society activity.

15 Developing Telecoms. (2026, April 14). Gabon announces tough restrictions on social media use. Developing Telecoms. https://developingtelecoms.com/telecom-business/telecom-regulation/20109-gabon-announces-tough-restrictions-on-social-media-use.html

Gap 4: The Participation and Evidence Deficit

Children remain absent from the design of policies intended to protect them. The majority of legislative processes lack structured mechanisms to hear from children or communities most affected by online harms. Also, outside of the UNICEF/ECPAT/INTERPOL Disrupting Harm studies (covering 13 countries in Eastern and Southern Africa), there is limited Africa-specific research on the scale, nature, and drivers of online harms to children.

Gap 5: Digital Literacy and Prevention

The legislative framework is reactive by design. Child online safety requires a preventive dimension: equipping children, parents, educators, and communities with the knowledge and skills to navigate digital environments safely. While several strategies mention digital literacy, systematic integration of digital safety education into school curricula remains absent across most of the continent.

4. Drivers and Barriers to Implementation Progress

4.1. Drivers

In every country with an advanced framework, three enabling factors are evident:

- **International organisations:** Organisations such as UNICEF, the Council of Europe and the ITU have played a catalytic role.
- **Institutional champions with mandates and political will:** Ghana's CSA, Kenya's Communications Authority, Cameroon's ANTIC, Zambia's ZICTA, South Africa's FPB are examples here. Advocacy that identifies and supports institutional champions is more effective than campaigns directed at "government" broadly.
- **Coalition pressure:** Direct support and partnerships with multi-stakeholder coalitions and civil society organisations serving as technical partners generate the broadest political support.

4.2. Barriers

- **Competing legislative priorities:** Child online safety competes for bandwidth with issues perceived as more immediately pressing. Advocacy must frame COP as a child protection, public health, and economic productivity concern, not a niche digital issue.
- **Regulatory capture and platform lobbying:** Platform accountability provisions are the most politically contested elements of COP (and, in fact, many digital-related) legislation. As African markets grow in commercial significance, the risk of regulatory capture increases.
- **Surveillance and rights concerns:** Uganda's experience is instructive: the Computer Misuse (Amendment) Act 2022 included provisions on children's data but was widely criticised, and the Constitutional Court struck down several sections in March 2026. The same goes for the Nigerian Cybercrime Act pre-amendment and South Sudan's Cybercrimes Act 2026.

  Poorly designed COP legislation risks being weaponised. The Uganda, Nigeria and South Sudan precedents underscore that advocacy for COP legislation must insist on rights-respecting design or risk building instruments that harm the people they're intended to protect.

5. Advocacy Recommendations

5.1. Civil Society Organisations

1. Prioritise domestication of the AU COP Policy

The AU COP Policy provides a continental mandate. Civil society should develop country-specific domestication roadmaps that translate the Policy's action areas into concrete legislative proposals tailored to each country's existing legal architecture. Priority should go to countries with functioning DPAs and data protection regulations.

2. Build a national COP coalition modelled on Nigeria's approach

Forming coalitions and volunteering to serve as technical partners can prove effective in getting legislation through. It's important that these coalitions and technical support are available from the draft stage, and especially in countries with partial frameworks that could be strengthened.

3. Use DPAs as strategic entry points

In countries where dedicated COP legislation faces political headwinds, DPAs offer an alternative pathway. The Mali and Senegal precedents, where DPA directives specifically address children's data, demonstrate that existing mandates can be leveraged. Civil society should engage DPAs systematically.

4. Insist on rights-respecting design

Uganda's constitutional crisis and CPJ's concerns about South Sudan's Act are warnings. COP legislation must include clear scope limitations, proportionality requirements, judicial oversight, and explicit protections for freedom of expression.

Model Legislation Checklist



- Does the law define "harmful content" with specificity sufficient to prevent arbitrary enforcement?
- Are platform obligations proportionate and technically feasible?
- Is the enforcement authority subject to independent judicial oversight?
- Are freedom of expression and access to information explicitly protected?
- Are children's participation rights (not just protection rights) addressed?
- Does the framework include transparency and accountability mechanisms for the regulator?
- Is there a sunset or review clause?

5.2. For the African Union and Regional Economic Communities

1. Develop an AU COP Policy implementation scorecard

An annual or biennial scorecard made publicly available would create positive competitive pressure and enable the identification of laggard states. It should cover legislative adoption, institutional capacity, enforcement activities, and child participation metrics.

2. Leverage RECs for sub-regional harmonisation

Regional economic communities remain relevant. ECOWAS should develop a directive on child online safety. The EAC should integrate COP into digital economy protocols. SADC should extend its Model Law approach. Harmonised standards reduce the regulatory arbitrage that platforms exploit.

5.3. For International Development Partners and Donors

1. Fund implementation, not just legislation

Legislation is the easier part; implementation is where frameworks fail. Partners should shift investment toward institutional capacity-building: digital forensics, specialised investigator training, prosecutor capacity, and judicial training.

2. Commission Africa-specific evidence

The Disrupting Harm studies remain the most rigorous evidence base but cover only a subset of countries. Updated, expanded research covering Francophone and Lusophone Africa, North Africa, and emerging threats (AI-generated CSAM, deepfakes, sextortion) is urgently needed.

3. Support platform accountability mechanisms

Development partners should fund technical capacity for African regulators in algorithmic auditing, content moderation review, and age-verification standards.

5.4. For Technology Platforms

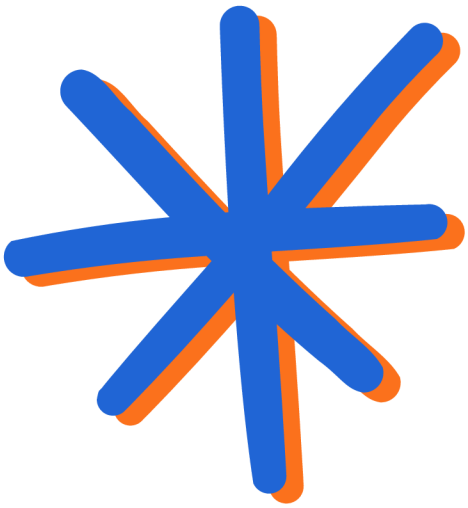
1. Apply global standards uniformly

Platforms should apply their highest child safety standards uniformly across all markets. Platforms should extend features deployed for European markets under the DSA or UK Online Safety Act to African users without waiting for local regulatory mandates.

2. Invest in African-language content moderation

Content moderation capacity for African languages remains grossly inadequate. Platforms should invest in native-language moderation for major African languages, train AI models on African-language CSAM and grooming patterns, and establish regional trust and safety teams with genuine decision-making authority.

Strategic Priorities: Where to Focus First



High Impact/High Feasibility

- **Nigeria:** Push HB.244 through the Senate and to presidential assent. The coalition infrastructure exists, and the political momentum is real.
- **Kenya:** Monitor and support implementation of COP Guidelines (binding on licensed providers). Advocate for consolidation into primary COP legislation.
- **South Africa:** Advocate for a standalone COP law that consolidates existing protections under the FPA, Cybercrimes Act, POPIA, and Children's Act.
- DPA engagement: In countries with functioning DSAs, formally charge DSAs to pay attention to rule-setting around child online protection while laws are still being developed.

High Impact/Medium Feasibility

- **Rwanda:** Support finalisation of primary COP legislation, building on the existing ministerial order and COP Policy.
- **Malawi:** Support MACRA in finalising the National COP Strategy and associated regulations.
- **Ethopia:** Build on the February 2026 UN CRC Committee recommendations to push for dedicated COP policy/legislation.
- **Zambia:** Support implementation of the NCOP Strategy 2025–2029; advocate for legislative backing.
- **ECOWAS:** Advocate for a sub-regional directive on child online safety.

Long-Term/Structural

- AU COP Policy scorecard development and monitoring.
- Francophone and Lusophone Africa evidence generation (Disrupting Harm expansion).
- Continental model legislation.
- Rights-impact assessments for recently enacted cyber laws (South Sudan, Liberia) to identify risks of misuse.

6. Conclusion

Africa is at an inflexion point on child online safety. The AU's continental policy, the cluster of legislative and regulatory advances in 2023–2025, and the growing engagement of data protection authorities and national strategies signal genuine momentum. But the continent's experience with cybercrime legislation shows that the path from adoption to implementation is where most reform agendas stall and often produce unintended consequences.

The advocacy challenge now is threefold: to ensure that adopted legislation is rights-respecting and technically sound; to build institutional capacity for enforcement; and to address the structural power asymmetry between African regulators and global technology platforms. This requires sustained, coordinated, evidence-informed advocacy, coalition-building that includes children as participants, and an honest reckoning with the tension between protection and rights.

References

African Union. (2024, February). The African Union child online safety and empowerment policy. African Union Commission.

Accessible Law. (n.d.). Children. POPIA: Protection of Personal Information Act. Retrieved June 8, 2026, from https://popia.co.za/category/children/

Communications Authority of Kenya. (2025, April). Industry guidelines for child online protection and safety in Kenya. Communications Authority of Kenya. https://www.ca.go.ke/sites/default/files/2025-04/%20Industry%20Guidelines%20for%20Child%20Online%20Protection%20%28COP%29%20and%20Safety%20in%20Kenya_Apr2025.pdf

Council of Europe. (2025, January 15). Rwanda becomes the 78th Party to the Convention on Cybercrime and accedes to the First Protocol. Cybercrime Programme Office. https://www.coe.int/en/web/cybercrime/-/rwanda-becomes-the-78th-party-to-the-convention-on-cybercrime-and-accedes-to-the-first-protocol

Cyber Security Authority. (2024). National child online protection framework. Government of Ghana. https://www.csa.gov.gh/resources/National%20COP%20Framework.pdf

Developing Telecoms. (2026, April 14). Gabon announces tough restrictions on social media use. Developing Telecoms. https://developingtelecoms.com/telecom-business/telecom-regulation/20109-gabon-announces-tough-restrictions-on-social-media-use.html

Emejo, J. (2026, May 27). Experts urge Senate to speed up passage of child online safety bill amid rising digital threats. ThisDay. https://www.thisdaylive.com/2026/05/27/experts-urge-senate-to-speed-up-passage-of-child-online-safety-bill-amid-rising-digital-threats/

Information and Communication Technologies Authority. (2025, December 1). Telecommunication Directive 4 of 2025 (TD 4 of 2025): Child online protection measures. Government of Mauritius. https://www.icta.mu/documents/2025/12/TD_4_of_2025.pdf

International Telecommunication Union. (2020). Child online protection guidelines. International Telecommunication Union. https://www.itu-cop-guidelines.com/

Paradigm Initiative. (2024, June). Malawi country report (Londa Digital Rights and Inclusion in Africa Report 2023/2024). Paradigm Initiative. https://paradigmhq.org/wp-content/uploads/2024/06/Malawi-Country-Report.pdf

Senior Reporter. (2026, June 3). Zimbabwe approves landmark child online protection policy as digital risks to children grow. The Besana Mail. https://thebesanamail.com/2026/06/03/zimbabwe-approves-landmark-child-online-protection-policy-as-digital-risks-to-children-grow/

References

UNICEF. (n.d.). How many children are there in Africa? UNICEF Data. Retrieved June 8, 2026, from https://data.unicef.org/how-many/how-many-children-under-18-are-there-in-africa/

UNICEF Zambia. (2024, October 11). Children request investments in digital literacy and child-friendly reporting mechanisms. UNICEF. https://www.unicef.org/zambia/press-releases/children-request-investments-digital-literacy-and-child-friendly-reporting

African Union. (2014, June 27). African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). African Union. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

This policy brief is based on the Digital Initiative for Innovation and Development (DIID) "Child Online Safety Policy Landscape Across African Countries Mapping (May 2026)" and publicly available verified information.

Digital Initiative For Innovation & Development

5th Floor, Murjanatu House, 1 Zambezi Crescent, off Aguyi Ironsi Street, Maitama, Abuja.

Web diidinitiative.org **Email** hello@diidinitiative.org @DiidOfficial