Kenya Red Cross

ICHA International Center for Humanitarian Affairs
At the Kenya Red Cross Society
• Inquire • Understand • Influence

SlovakAid
GOOD IDEA SLOVAKIA

SLOVAK AGENCY FOR INTERNATIONAL DEVELOPMENT COOPERATION

Governing Artificial Intelligence in Humanitarian Action in Kenya

Advancing Responsible, Ethical and Inclusive AI

POLICY BRIEF

Executive summary

Artificial intelligence (AI) is already changing how humanitarian work is done, across the sector and increasingly in Kenya. Forecasting and early-warning models help agencies anticipate droughts and floods and act before a crisis peaks. Satellite imagery and geospatial analysis speed up damage and needs assessments, while data tools support faster registration, targeting and delivery of cash assistance at scale. Chatbots, translation and speech tools let organizations reach communities in local languages and respond to feedback faster, and generative AI is cutting the time spent on reporting, analysis and information management. Used well, AI helps humanitarians reach more people, faster and with fewer resources. But the speed and scale that make AI valuable also magnify the harm when it goes wrong, and the rules have not kept up.

Humanitarian organizations in Kenya now use artificial intelligence (AI) in their daily work. Governance has not kept pace. A global survey of 2,539 humanitarians by the Humanitarian Leadership Academy (HLA) and Data Friendly Space (DFS) shows the gap: 70% use AI daily or weekly, but only 22% of organizations have formal AI policies.[1]

The gap matters because AI in humanitarian action affects people who have little ability to opt out. A biased targeting model, a breached beneficiary database or an unchallengeable automated decision can cost someone their assistance or expose them to harm. Kenya's Data Protection Act 2019, the Computer Misuse and Cybercrimes Act 2018 and the National AI Strategy 2025-2030 provide a foundation.[2] None of them sets out how AI should be governed in humanitarian operations.

The Humanitarian Framework for Responsible and Ethical Use of AI in Kenya responds to this gap by complementing existing guidance. It builds on ICRC, IASC and OECD guidance and Kenya's Data Protection Act, cyber laws and National AI Strategy, and turns them into practical controls for humanitarian operations. It applies a four-tier risk classification and minimum controls for each tier. It defines lifecycle accountability roles, an appeal and redress mechanisms , and a list of some prohibited AI uses. In doing so, it lays a shared foundation for how Kenya's humanitarian sector adopts and uses AI, one that organisations can build on together and that can inform national AI policy and law as they develop.

Key policy messages

- **Coordinate governance.** Kenya needs a single humanitarian AI framework that every organization applies, with common risk tiers, safeguards and prohibited uses. National AI policy and law should recognize it as the sector reference and classify AI used for humanitarian eligibility, targeting and biometric identification as high-risk.
- **Secure the AI lifecycle.** Build cybersecurity and data protection controls into every AI system that processes beneficiary data, including systems from third-party vendors.
- **Protect affected people.** Guarantee meaningful human oversight, bias testing, non-digital alternatives and accessible redress for consequential decisions.
- **Build capacity and buy responsibly.** Train staff on AI risks, bring unsanctioned "shadow AI" tools under approval, and set standard procurement clauses.
- **Monitor and learn as a sector.** Make AI incident tagging, out-of-cycle reviews and shared learning with regulators routine practice.

1 Humanitarian Leadership Academy & Data Friendly Space. (2025). How are humanitarians using artificial intelligence in 2025? Mapping current practice and future potential: Full insights report. https://www.humanitarianleadershipacademy.org/wp-content/uploads/2025/08/Full-insights-report-How-are-humanitarians-using-AI-in-2025.pdf

2 Data Protection Act, No. 24 of 2019 (Kenya). https://new.kenyalaw.org/akn/ke/act/2019/24 ; Computer Misuse and Cybercrimes Act, No. 5 of 2018 (Kenya). https://dig.watch/resource/kenyas-computer-misuse-and-cybercrimes-act-no-5-of-2018; Ministry of Information, Communications and the Digital Economy. (2025). Kenya national artificial intelligence strategy 2025–2030. https://ict.go.ke/sites/default/files/2025-03/Kenya%20AI%20Strategy%202025%20-%202030.pdf

The policy problem

The question is no longer whether AI will be used, but how, where, by whom and under what conditions. Recurrent humanitarian situations create a real need for faster analysis. Literature points to use across the whole crisis cycle: early warning, geospatial vulnerability mapping, logistics, needs assessment and information management.[3]

The stakes are higher in humanitarian settings than in most other sectors employing the use of AI. People in crisis depend on assistance, often cannot refuse data collection, and face power imbalances with those who hold their data.[4] When an AI system fails, the harm falls directly on them:

- Biased model or data: eligible households are scored out of assistance. Facial analysis systems show error rates of up to 34.7% for darker-skinned women, against 0.8% for lighter-skinned men.[5] Algorithmic cash targeting in Jordan excluded people in need.[6]
- Cyber incident (confidentiality, integrity, availability): a breach exposes the identities and locations of displaced people, a tampered model distorts who is prioritized, and an outage blocks registration or helplines.
- Unlawful or excessive data processing: sensitive and biometric data are reused, shared or sent abroad beyond what people consented to.
- Opaque, automated decisions: people cannot learn why they were refused help, or challenge the decision.
- Digital exclusion: people with poor connectivity, low literacy or limited language access are missed by digital-first services.

Cybersecurity and data protection must be governed together, but they are not the same thing. Cybersecurity protects systems and data from compromise; in Kenya it falls under the Computer Misuse and Cybercrimes Act 2018 (amended in 2025) and the National Cybersecurity Strategy 2022-2027.[7] Data protection governs whether personal data may lawfully be processed at all, under the Data Protection Act 2019 and the oversight of the Office of the Data Protection Commissioner (ODPC).[8] A system can be secure and still unlawful, or lawful and still insecure. For crisis-affected people, a failure of either is a protection failure, not only an information technology (IT) failure.

What the evidence shows

Published evidence, from a global survey of humanitarian practitioners, academic research and existing international guidance, points to three findings that matter most for policy. Each is set out below with its evidence base and policy implication.

Use is outpacing governance. Globally, 70% of institutions operating in the humanitarian sector use AI daily or weekly, but only 22% of organizations have formal AI policies. Source: HLA and DFS survey.[1] Implication: unsanctioned use of AI tools is the norm, so governance must cover everyday tools, not only flagship systems.

Specific risks are well documented. These are bias and exclusion, poor data quality and privacy, inaccurate AI-generated information, cybersecurity exposure, and erosion of human judgement.

3 Beduschi, A. (2022). Harnessing the potential of artificial intelligence for humanitarian action: Opportunities and risks. International Review of the Red Cross, 104(919), 1149–1169. https://doi.org/10.1017/S1816383122000261; Lythreatis, S., Acikgoz, F., & Yassine, N. (2026). Artificial intelligence in humanitarian aid: A review and future research agenda. Technovation, 151, Article 103415. https://doi.org/10.1016/j.technovation.2025.103415

4 Pizzi, M., Romanoff, M., & Engelhardt, T. (2020). AI for humanitarian action: Human rights and ethics. International Review of the Red Cross, 102(913), 145–180. https://doi.org/10.1017/S1816383121000011

5 Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, 81, 77–91. https://proceedings.mlr.press/v81/buolamwini18a.html

6 Toh, A. (2023). Automated neglect: How the World Bank's push to allocate cash assistance using algorithms threatens rights. Human Rights Watch. https://www.hrw.org/report/2023/06/13/automated-neglect/how-world-banks-push-allocate-cash-assistance-using-algorithms

7 Government of Kenya. (2022). National cybersecurity strategy 2022. https://interior.go.ke/sites/default/files/2024-05/L-897-KENYA-CYBERSECURITY-STRATEGY-6_220922_103959_220930_161437.pdf ; Computer Misuse and Cybercrimes Act, No. 5 of 2018 (Kenya). https://dig.watch/resource/kenyas-computer-misuse-and-cybercrimes-act-no-5-of-2018; Computer Misuse and Cybercrimes (Amendment) Act, 2025 (Kenya). https://hapakenya.com/wp-content/uploads/2025/10/The-Computer-Misuse-and-Cybercrimes-Amendment-Act-2025.pdf

8 Data Protection Act, No. 24 of 2019 (Kenya). https://new.kenyalaw.org/akn/ke/act/2019/24

Accountability is fragmented. Many tools come from external providers, which raises questions of data ownership and oversight. Existing guidance from the International Committee of the Red Cross (ICRC), the Inter-Agency Standing Committee (IASC), the Organization for Economic Co-operation and Development (OECD) and the European Union (EU) is largely non-binding and not cross-referenced, and it leans on data protection rather than model behavior.

Why Kenya needs the Humanitarian AI Framework

The Framework is designed to fill that space. It sets the conditions under which AI may be developed, procured or deployed in humanitarian action in Kenya. It is designed as "an operational and accountability layer" between high-level policy instruments and field operations. It rests on international humanitarian law, the Fundamental Humanitarian Principles, the Constitution, the Data Protection Act and the National AI Strategy.[9] The Framework has five core elements, summarised below: its principles, risk tiers, governance arrangements, monitoring and learning, and practical tools.

Principles. Do No Harm as the foundation. Eight principles under it: Inclusivity and Fairness, Meaningful Human Oversight, Integrity, Explainability, Sustainability, Resilience, Contextualisation and Data Governance. Resilience explicitly covers cyber threats, security testing and incident logging.

Risk tiers. Four tiers. Tier 1 (low, e.g. administrative drafting) needs standard controls. Tier 2 (medium) needs a documented assessment and a human review point. Tier 3 (high, e.g. eligibility, targeting, biometrics) needs a data protection impact assessment (DPIA), pre-deployment testing, human approval of individual decisions, quarterly review and redress. Tier 4 uses are prohibited. Preventative, detective and corrective controls scale with the tier.

Governance. A responsible, accountable, consulted and informed (RACI) matrix across the AI lifecycle. Named roles from AI System Owner to a Governance and Ethics Committee. Security controls including encryption, role-based access and vendor due diligence, plus safeguards for cross-border processing. AI incidents are tagged and graded by severity. The System Owner can suspend a system immediately.

Monitoring and learning. Indicators mapped to all eight principles. Out-of-cycle review after a model or vendor change, a security incident, evidence of bias or a complaint. Lessons shared with regulators and national AI governance processes.

Tools. A use-case assessment, a seven-stage lifecycle review and prohibited uses. Prohibited uses include biometric enrolment as a condition of aid, unappealable automated eligibility decisions, emotion recognition, and transferring beneficiary data abroad without safeguards.

The Framework complements Kenya's legal and policy architecture. It turns obligations that already exist, such as DPIAs under the Data Protection Act and security duties under cyber law, into concrete controls for humanitarian operations. It also prepares the sector for a likely AI law.[10] To work as the sector standard, it needs what no single organization can provide: cross-sector coordination, a national incident channel and regulatory recognition. The public action set out below would give it that backing.

Policy recommendations

Coordinate humanitarian AI governance. Accountability is fragmented, and only 22% of humanitarian organizations globally have formal AI policies.[1] Every humanitarian organization in Kenya should apply a single, shared humanitarian AI framework as the sector reference. Each should set up an AI governance or ethics committee, name an accountable owner for every AI system and keep an AI register. The Ministry of Information, Communications and the Digital Economy (MICDE) should convene a humanitarian AI working group that brings together ODPC, the national cybersecurity agencies, humanitarian actors, developers and civil society.

9 Ministry of Information, Communications and the Digital Economy. (2025). Kenya national artificial intelligence strategy 2025–2030. https://ict.go.ke/sites/default/files/2025-03/Kenya%20AI%20Strategy%202025%20-%202030.pdf

10 Parliament of Kenya. (2026). Bill digest: The Artificial Intelligence Bill (Senate Bills No. 4 of 2026). https://www.parliament.go.ke/sites/default/files/2026-04/Bill%20Digest%20-%20The%20Artificial%20Intelligence%20Bill%2C%20No.4%20of%202026.pdf

Build cybersecurity and data protection into the AI lifecycle. Cybersecurity exposure and privacy are among the main risks. Vendor and cross-border processing is poorly governed.

Humanitarian organizations, led by their Information Security Leads and Data Protection Officers, should complete a DPIA and security testing, including penetration testing, before deploying any high-risk AI system. They should apply encryption and role-based access, carry out due diligence on vendors, and include exit and data-deletion terms in vendor contracts. ODPC should issue sector guidance on DPIAs for humanitarian AI and, with the national cybersecurity authorities, agree a protocol that links AI incident reporting to national cyber incident-response channels.

Protect rights, fairness and redress. Bias, exclusion and erosion of human judgement can deny people assistance.

Humanitarian organizations should audit AI systems for bias and exclusion before go-live and require human approval of every high-risk decision. They should build appeals into existing feedback channels and keep a non-biometric, non-digital alternative for essential aid. Working with civil society and community representatives, they should involve communities, including women, persons with disabilities and displaced people, in validating high-risk systems, and publish plain-language AI notices in Kiswahili and local languages.

Build capacity, AI literacy and responsible procurement. Unsanctioned use is widespread, and tools are mostly procured from outside providers.

Humanitarian organizations should train staff on automation bias, approved uses and verification of AI outputs, and carry out procurement and legal due diligence on vendors. Together with MICDE, training institutions and local developers, the sector should develop model AI procurement clauses covering security, data reuse, audit access and exit, and agree an approved-tools list for generative AI.

Monitor, report incidents and keep learning. Benefits are not independently measured, and harms go untracked.

AI system owners should monitor systems in proportion to their risk, tag and grade AI incidents by severity, carry out out-of-cycle reviews when needed, and share lessons with regulators. Monitoring, evaluation, accountability and learning (MEAL) functions, research institutions and the working group should keep a shared, anonymized log of humanitarian AI incidents and lessons, and commission an independent mid-term review in 2029 and a full review in 2032.

Conclusion and call to action

AI can make humanitarian action faster and better targeted. Without safeguards, a security lapse, a biased model or an unchallengeable decision becomes harm to people who are already vulnerable. Kenya does not need to choose between innovation and protection. A single humanitarian AI framework, applied by every organization and recognized in national law, makes it possible to have both. We call on:

- Ministry of Information, Communication and the Digital Economy to convene a humanitarian AI working group, recognize a single humanitarian AI framework as the sector reference, and reflect humanitarian high-risk uses in national AI governance.
- ODPC and the national cybersecurity authorities to co-develop DPIA guidance and an incident-reporting protocol for humanitarian AI.
- Humanitarian organizations, donors and technology providers to adopt the Framework as their common standard, applying its assessments, prohibited-uses list and procurement standards, and to fund the capacity to apply them.

ICHA International Center for Humanitarian Affairs

At the Kenya Red Cross Society

• Inquire • Understand • Influence

Contact us:

info@icha.net

TEL: 0703 037 051

Office Location

Red Cross Road, Off Popo road, South C,

Nairobi, Kenya