DHRP Digital Health & Rights Project

KELIN Reclaiming Rights, Rebuilding Lives

KCAT KENYA COMMUNITY ADVISORY TEAM

POLICY BRIEF

The Future of Human Rights in the Digital Age: Youth Perspectives on Digital Empowerment, Inclusion, and Governance in Kenya

01 Background

Kenya stands at the forefront of the digital revolution in Sub-Saharan Africa, driven by rapid technological innovation and high internet penetration, estimated at 92%.[1] Factors such as affordable smartphones, improved infrastructure, and government strategies like the National Broadband Strategy have accelerated digital adoption. With over 60% of the population under 25, the country is poised for a tech-driven transformation in all sectors, particularly the healthcare sector.

However, **while young people increasingly access health services and information online,** they are rarely involved in shaping the policies governing their data collection and use.[2] Kenya's digital revolution presents critical opportunities and challenges in ensuring the accessibility, availability, and quality of health for all.

First, despite high internet penetration (92%) and mobile device use accounting for 72% of web traffic,[3] **digital divides persist**, especially for women, rural populations, persons with disabilities, and low-income groups. For instance, while mobile ownership is widespread, access to smartphone-based apps remains limited, excluding millions who cannot afford them.[4]

[1]We Are Social & Meltwater (2023), "Digital 2023 Kenya," Retrieved from https://datareportal.com/reports/digital-2023-kenya on 01 December 2023.

[2]Wong, B. L. H., Smith, R. D., Siepmann, I., Hasse, A., & Tandon, S. (2021). Youth engagement in digital health: a critical perspective towards meaningful youth agency in governance. MMS Bull, 157.

[3]Natalie , Cowling (2023). Web traffic by device in Kenya 2023, In Statista - The Statistics Portal. Retrieved from https://www.statista.com/statistics/1312186/web-traffic-by-device-in-kenya/ .

[4]Gebayew, C., Hardini, I. R., Panjaitan, G. H. A., & Kurniawan, N. B. (2018, October). A systematic literature review on digital transformation. In 2018 International Conference on Information Technology Systems and Innovation (ICITSI) (pp. 260-265). IEEE.

Second, although **digital health tools and AI offer potential to transform health systems**, they also **raise serious human rights concerns**. These include risks to privacy, autonomy, equality, and sovereignty[5], as well as algorithmic bias, data colonialism, and weak data protection that can lead to surveillance and targeting.[6]

Third, digital platforms offer crucial access to health information and services for stigmatized and criminalized groups, enhancing reach and reducing barriers[7]. Yet, **digital harms**—such as online violence, surveillance, and misinformation—pose new threats. Many prefer to remain "uncounted" in health studies due to fears of exposure and criminalization.[8]

Fourth, Kenya has made strides in digital health governance, through frameworks such as the National eHealth Strategy (2011–2017), the National eHealth Policy (2016–2030), the Digital Health Act (2023) and the Data Protection Act (2019). However, **meaningful participation**, especially by marginalized groups, is still lacking in the design and implementation.

In 2022, UN leaders reaffirmed that human rights must be central to tech governance.[9] The HIV movement offers valuable lessons in asserting privacy, non-discrimination, and accountability through community-led approaches.

This policy brief summarises recommendations from a study conducted by the Digital Health and Rights Project (DHRP)[10] in Kenya (led in Kenya by the Kenya Legal and Ethical Issues Network on HIV and AIDS (KELIN) and Warwick University). The study examined how young people living with HIV (PLHIV), young female sex workers, and young LGBTQ+ individuals navigate digital spaces, focusing on empowerment, inclusion, and governance from a human rights perspective. Employing a participatory action research (PAR) approach, the study engaged 109 participants aged 18–30 across Nairobi, Mombasa, Kitui, and Migori counties, selected for their diverse geographic and demographic profiles, internet penetration and key population organizations. Data was collected through focus group discussions (FGDs), semi-structured key informant interviews (KIIs), and legal/policy analysis, ensuring meaningful involvement of youth, including key populations. Ethical considerations prioritized participant anonymity, informed consent, and protection from stigma and harm.

[5]Martens, B. (2018). The importance of data access regimes for artificial intelligence and machine learning; Anand, P. (2022). Governing Virtual Space: Analysing Internet Access As A Human Right In The Age Of Information. Journal of Positive School Psychology, 6(2), 1575-1586.

[6]UN Human Rights Office. 2020. "Emerging digital technologies entrench racial inequality, UN expert warns, 15 July, Retrieved from https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=26101&La; Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019. Profile books; Couldry, N., & Mejias, U. A. (2019). Data colonialism: Rethinking big data's relation to the contemporary subject. Television & New Media, 20(4), 336-349

[7]Dasgupta, R. K. (2015). Digital media & the Internet for HIV prevention, capacity building & advocacy among gay, other men who have sex with men (MSM) & transgenders: Perspectives from Kolkata, India. Edited by Christopher S Walsh, 65.

[8]Davis, S. L., Esom, K., Gustav, R., Maleche, A., & Podmore, M. (2020). A democracy deficit in digital health?. Health and Human Rights Journal. Retrieved from https://www.hhrjournal.org/2020/01/a-democracy-deficit-in-digital-health/.

[9]The Office of the High Commissioner for Human Rights, (2022). Human rights should be at the heart of tech governance. Retrieved from https://www.ohchr.org/en/stories/2022/09/human-rights-should-be-heart-tech-governance

[10]The Digital Health and Rights Project, established in 2019, is a global consortium of researchers, activists, and organizations advocating for human rights in digital health. It includes partners from Kenya, Colombia, Vietnam, Ghana, the UK, and beyond.

02 Summary of Findings and Policy Recommendations

a. Findings on Barriers to Digital Inclusion

Barriers to digital inclusion are the obstacles that prevent individuals and communities from fully accessing, using, and benefiting from digital technologies and online resources. Our findings identified three primary categories of barriers that hinder young people's involvement in accessing health information on digital platforms including **stigma, economic hardship, and educational/cultural constraints.**

Stigma

- Stigma remains a significant barrier to achieving digital inclusion. It manifests as the fear of judgment, discrimination and potential exposure, often stemming from entrenched societal norms and perceived digital surveillance.
- Participants reported that they had withdrawn from digital platforms due to abuse, violations of privacy, and fear of being judged based on their health status, sexual interests and/or identities.

Stigma leads to digital self-censorship, increased mental health risks, and disengagement from digital platforms, especially for those whose identities or health conditions face social stigma.

Economic Hardship

- Economic barriers to digital services encompass a range of financial constraints that prevent individuals, especially young people, from accessing and utilizing digital technologies and platforms.
- Participants described a range of economic challenges, including the inability to afford smartphones, limited funds to buy data and or internet access, dependence on others like parents or partners for devices or airtime and in other cases, resorting to borrowing just to stay connected. These conditions not only restrict digital participation but also limit young people's autonomy, confidentiality, and access to vital health resources.

Economic constraints prevent many from the digital world due to the high costs of devices, and data, further widening the digital divide and reinforcing cycles of poverty.

Education/Cultural Barriers

- Educational and cultural barriers greatly impede young people's ability to access sexual and reproductive health and related information from digital platforms. These barriers are influenced by a mix of inadequate formal education, limited digital literacy, and entrenched cultural and religious beliefs that discourage open discussion about digital tools and online health information.
- Barriers related to education are significantly shaped by stigma, misinformation, and cultural norms. Participants highlighted how fear, stigma, and lack of exposure to

digital technologies prevent many from seeking health information online. Cultural taboos and perceived gender roles also create environments where discussing health issues, particularly those related to sexuality or identity, is discouraged.

Educational and cultural barriers restrict digital participation, breeding distrust of online platforms, and perpetuating exclusion, especially where societal norms limit the expression or use of digital tools.

03 Policy Recommendations to Ensure Digital Inclusion

a) Address stigma and promote safe digital spaces

- The Office of the Data Protection Commissioner (ODPC) should strengthen the enforcement of the Data Protection Act (2019) to safeguard user privacy and build trust in digital health platforms.
- Ministry of Health (MoH) should integrate anti-Stigma safeguards into digital health strategies and in implementation, ensuring that online health services are inclusive and respectful of all users.
- Communications Authority of Kenya (CA) should require digital platforms and service providers to implement accessible reporting mechanisms for online harassment, cyberbullying, and privacy violations.
- National mental health strategies should incorporate digital psychosocial support services, including toll-free helplines, online counselling, and peer support platforms, to address the mental health impacts of stigma-driven digital exclusion.

b) Reducing Economic Barriers to Digital Access:

- The Ministry of ICT and the Digital Economy should implement programs to increase access to affordable internet services and digital devices, particularly targeting youth populations.
- Digital connectivity should be formally integrated into youth empowerment and social protection programs at both the National and County Government levels, ensuring equitable access for all young people.

c) Addressing Educational and Cultural Barriers

- The Ministry of Education should integrate age-appropriate digital literacy into formal and non-formal learning systems - emphasising safe internet use, critical evaluation of online information, and accessing credible digital health resources.
- Government and development partners should institutionalize youth-led digital literacy and peer education programs, recognizing young people as key agents of change in reducing stigma and increasing uptake of digital health platforms.

d) Strengthen coordination between the Ministry of ICT, Ministry of Health, Ministry of Education, and county governments to ensure coherent implementation of digital inclusion policies.

e) Institutionalize Meaningful Youth Participation - Ensure young people are meaningfully involved in the design, implementation, and evaluation of digital inclusion and digital health policies, recognizing their insights, experiences, and needs as critical to effective and equitable digital governance.

04 Findings on Digital Safety and Privacy

- Digital safety and privacy describe the ability to navigate the internet, use devices, and exchange information without undue risk of surveillance, coercion, or exposure.
- Participants across all four counties reported how everyday digital activities including receiving clinic reminders, joining WhatsApp groups, or searching for health content, could result in blackmail, stigma, and social isolation. These threats are compounded by shared devices, unsecured networks, and opaque data practices.
- Young people reported the risks of involuntary outing, social isolation, psychological distress, and loss of income. This leads to avoidance of digital health services due to fear of being tracked or exposed.
- Strengthening data protection, digital literacy, and accountability mechanisms is therefore critical to safeguarding young people's rights in an increasingly networked health landscape.

Surveillance (family and friend, private company and government)

- Participants described how risks inherent in phone sharing, fear of remote hacking, and unauthorized monitoring on platforms including WhatsApp, Facebook, and dating apps affected their participation in digital platforms. Tools like WhatsApp Web, app tracking, and national health or biometric systems were frequently cited.
- Young women, LGBTQ+ individuals, and persons living with HIV were often vulnerable to the intrusions resulting in involuntary disclosure of HIV status, sexual orientation, gender identity, and financial details. These breaches resulted in blackmail, stigma, emotional distress, denial of services and a withdrawal from digital health platforms.

Technology Facilitated Abuse

- Technology-facilitated abuse (TFA) is defined as abuse that is committed, assisted, aggravated or amplified using internet and communication technologies or other digital technologies, that results in or is likely to result in physical, sexual, psychological, social, political or economic harm, or other infringements of rights and freedoms. It ranges from cyber-bullying, stalking, and account hijacking to blackmail and the non-consensual sharing of intimate images.
- Participants described instances of online stalking, blackmail, account takeovers, cyberbullying, and non-consensual sharing of intimate content. Most reports came from female participants, but abuse spanned every gender identity and all the four counties, turning phones, public Wi-Fi, WhatsApp, Facebook, TikTok, and Twitter into spaces of danger rather than support. Harms ranged from involuntary HIV disclosure and public shaming to lost livelihoods and suicidal thoughts.

Poor Data Protection

- Poor data protection describes an environment where personal information is collected, stored, and shared without clear safeguards, user consent, or effective oversight.
- Participants described how weak data safeguards exposed their health, identity, and creative work online. Across the board, poor data protection was seen as a key enabler of digital surveillance, technology-facilitated abuse, stigma, and unwanted exposure.
- Participants pointed to unchecked third-party data sharing, the impossibility of tracing how their information is used, and the absence of clear channels for reporting breaches.

- Unsecured SMS reminders that reveal HIV status, auto-filled sensitive searches, and leaked creative content all highlighted how privacy failures erode trust in digital services and public systems.

05 Policy Recommendations to Ensure Digital Safety and Privacy

a) Address Digital Surveillance and Unauthorised Monitoring

- The Office of the Data Protection Commissioner (ODPC), in collaboration with the Communications Authority of Kenya (CA), should enhance oversight of digital surveillance by state and non-state actors.
- Clear restrictions should be enforced on data collection, biometric systems, and monitoring tools used in health, telecommunications, and social protection programs, ensuring compliance with principles of necessity, proportionality, and informed consent under the Data Protection Act.
- The Ministry of ICT and MoH should issue guidelines for secure and confidential digital health communications, including discreet notifications, opt-in messaging, and alternatives to SMS for sensitive health information.

b) Prevent and Respond to Technology-Facilitated Abuse (TFA)

- Legal and policy responses should explicitly recognize technology-facilitated abuse as a form of gender-based violence (GBV), ensuring clarity, enforceability, and alignment with existing national and county GBV prevention and response mechanisms. Survivors of online abuse should be entitled to the same protections, support services, and legal remedies as those experiencing offline violence.
- Policies and interventions should recognize the interconnected and intersectional nature of technology-facilitated abuse, which affects diverse populations, including women, men, gender-diverse individuals, people living with HIV, sex workers, and men who have sex with men, and often links online harassment with offline violence and discrimination.
- A survivor-centred approach should guide all prevention and response efforts, upholding the right to privacy, dignity, and autonomy, and ensuring timely access to comprehensive support services, including medical care, mental health care, psychosocial support, and justice.
- The Communications Authority (CA), Office of the Data Protection Commissioner (ODPC), and law enforcement agencies should establish confidential, accessible and youth-friendly reporting mechanisms for digital abuse. These mechanisms should include simplified reporting channels, protection from retaliation, and clear referral pathways to psychosocial, legal, and health support services.
- The Government should ensure that social media companies and digital service providers operating in Kenya implement stronger content moderation systems, rapid response systems, and transparent appeal processes for abuse cases, ensuring timely and effective protection for users.

c) Strengthening Data Protection and Trust in Digital Systems

- The Ministry of Health (MoH) and Ministry of ICT should require all digital health systems to adopt privacy-by-design and privacy-by-default principles including data minimizing, encrypted communications, restricted third-party data sharing, and secure storage of sensitive health information.

- Policies should require all digital health and public service platforms to provide clear, accessible mechanisms for reporting data breaches and privacy violations, with guarantees of timely notification, investigation, and effective remedies for affected users.

d) Strengthen Inter-Agency Coordination between ODPC, CA, MoH, law enforcement, and county governments on digital safety and privacy enforcement to ensure effective, consistent enforcement of digital safety and privacy protections.

06 The Need for Digital Awareness and Empowerment

- Digital awareness and empowerment among young people in the context of health and rights refers to the ability to access, understand, and make use of digital platforms for health-related information, all while safeguarding one's rights and wellbeing in online environments.
- This concept goes beyond the basic access to also include the skills needed to navigate technology effectively, make informed health decisions, and exercise agency in digital environments.
- As digital tools become increasingly available, especially among young people in Kenya, digital engagement has emerged as a primary method of obtaining health information.
- While digital spaces provide youth with a means of autonomy and empowerment, this study reveals that many still encounter digital exclusion, unsafe environments, and limited participation in shaping the tools that impact their health.
- Therefore, meaningful investment in digital literacy, digital health literacy and digital rights and security literacy is crucial in promoting equity, inclusion, and agency among Kenya's digitally connected yet underserved youth.

Digital Literacy

- Overall, digital literacy-related barriers were prominent as participants noted this as a crucial barrier to digital engagement. These included difficulties with device use, navigating online content, identifying credible health sources, and engaging in safe online practices.

Digital Health Literacy

- Overall, digital literacy-related barriers were prominent as participants noted this as a crucial barrier to digital engagement. These included difficulties with device use, navigating online content, identifying credible health sources, and engaging in safe online practices.
- Many young people rely on platforms like TikTok and Facebook for health content, yet struggle with misinformation, judgment, or inability to discern reliable sources. In Nairobi and Mombasa counties digital health literacy was reported as a crucial barrier, with trans and non-binary individuals facing unique vulnerabilities due to stigma and lack of representation in digital health ecosystems.

Digital Rights and Security Literacy

- Participants highlighted critical gaps in understanding digital rights and data security - fear of surveillance, data misuse, and exposure of private information especially for key populations has created a culture of self-censorship and digital retreat.

07 Policy Recommendations: Advancing Digital Awareness and Empowerment Among Young People in Kenya

a) Strengthen Digital Literacy for Meaningful Participation

- The Ministry of Education, in collaboration with the Ministry of ICT and Digital Economy, should strengthen and standardize digital literacy education within the formal and non-formal learning systems, moving beyond basic device use to include navigation of online platforms, critical thinking, identifying credible information, and safe online practices.
- County governments should support inclusive community-based digital literacy programs targeting out-of-school youth, residents of informal settlement, and marginalized groups, with youth centers, libraries, and community hubs resourced to provide practical, hands-on digital skills training.

b) Mainstream Digital Rights Education Across Youth Programs

- The Ministry of ICT, ODPC, and Ministry of Youth should mainstream digital rights and data protection education within youth empowerment, health, and civic education programs ensuring youths understand their rights under the Data Protection Act (2019), including consent, data access, correction, and redress.
- Policies should support training on practical digital security measures, including privacy settings, secure communication, protection from surveillance, and safe use of shared devices, with particular attention to key populations facing heightened risks of exposure and harm.
- Young people should be informed about accessible channels for reporting digital abuse, data breaches, and rights violations, with awareness initiatives clearly outlining the roles of institutions such as the ODPC, CA, and law enforcement agencies in protecting digital rights.

Conclusion

To achieve an inclusive and equitable digital future, Kenya must decisively adopt rights-based digital governance that places privacy, digital literacy, and meaningful youth participation at its core. This demands firm enforcement of data protection laws, deliberate co-creation of youth-centred digital literacy initiatives, and the systematic integration of privacy-by-design principles across digital health platforms.