USAID
FROM THE AMERICAN PEOPLE

Digital Threats to Democracy in the Education Sector



Digital threats to democracy are a growing topic of conversation among those in the Democracy, Human Rights and Governance (DRG) sector. However, digital threats affect all USAID sectors, including economic growth, agriculture, education and global health. As noted in USAID's Digital Strategy, the increased use of digital tools and technology has brought many opportunities for improved outcomes in USAID partner countries. However, technology also provides an avenue for undemocratic actors to manipulate information, exploit private data, surveil public space, and impinge upon human rights. Building on the findings of the Bureau for Africa's 2021 Democratizing Digital Landscape Assessment, USAID has identified an important need and opportunity to further integrate awareness of digital threats to democracy into its programming. A 2022 digital development portfolio mapping of USAID digital development efforts showed that safeguards to protect privacy, human rights, and democratic freedoms are underrepresented and underreported in USAID-funded projects. This underscores the importance of countering and mitigating digital threats to democracy across USAID programming in sub-Saharan Africa. This document looks into the intersection of digital threats to democracy and the education sector for a USAID audience with an Africa focus. It offers recommendations for strategically raising awareness of digital threats to democracy and incorporating these considerations into programming, and explores key trends in digital threats to democracy across the education sector.

How USAID Can Mitigate Digital Threats to Democracy in its Education Sector Programming

The US Government Strategy on International Basic Education underscores the importance of digital tools in the education sector, stating that technology "can reduce cost and improve effectiveness, resulting in expanded access to quality education and improved learning outcomes." Similarly, USAID's Education Policy states that "Incorporating relevant information and communication technologies (ICTs) in education interventions can enhance the training and coaching of teachers and instructors; enable teachers and instructors to be more effective; aid in reaching marginalized and vulnerable children, including children with disabilities; and improve the collection and use of educational data to strengthen systems and improve policy decision-making." Yet while digital tools can help children and youth acquire critical skills and knowledge, they also present important digital risks and digital threats to democracy, such as increased digital surveillance in schools. Identifying and mitigating these threats across USAID's education portfolio supports the safety and integrity of educators, students, and parents while promoting open, inclusive, and secure digital ecosystems in USAID partner countries.

USAID can play an important role in fighting and mitigating digital threats to democracy through its education portfolio. The box below highlights key questions to consider during program design. This is followed by specific recommendations for USAID staff based in Washington and USAID Mission staff and implementing partners aiming to address these issues in their education programming.

Ensuring the use of rights-respecting technologies in USAID global health programming

Digital tools can accelerate development outcomes in USAID partner countries, but they can also pose digital threats to democracy. These threats may not be immediately clear. In considering the range of potential digital threats to democracy in the short- and long-term stemming from digital interventions in global health programming (digital tools, technologies, policies, processes, systems, or other digital ecosystem-oriented interventions), ask the following questions considering three scenarios:

1. impact under the current government,
2. impact if the current government begins or accelerates the process of democratic backsliding, and
3. impact under a new, more authoritarian government.

Questions for consideration:

- How can this intervention promote or be affected by **digital surveillance**?
- How can this intervention promote or be affected by **misinformation, disinformation, or malinformation**?
- How can this intervention promote or be affected by **online censorship**?
- How can this intervention promote or be affected by **internet shutdowns**?
- How can this intervention promote or be affected by **targeted online persecution**?
- How can this intervention promote or be affected by **offline persecution for online behavior**?
- How can this intervention potentially expose individuals to t**argeted harassment or legal issues** based on their gender, identity, or perceived affiliation with a group such as LGBTQI+?
- How can this intervention be positively or negatively affected by **data localization**?
- What are **other potential misuses of this intervention**?

Recommendations for USAID/Washington staff

These recommendations address how USAID/Washington staff can raise awareness of digital threats to democracy within their sectors and USAID portfolios - in this case, education.

Internal-facing

Develop guidance for USAID staff and implementing partners on how to apply the Donor Principles for Human Rights in the Digital Age to programming in the education sector. This will help ensure that USAID does not fund non-rights-respecting technologies.

Design and provide practical, hands-on training to USAID staff and implementing partners on:

- The risk of digital threats to democracy in the education sector, with a focus on concrete strategies to identify and mitigate potential digital rights abuses in their programming.
- Assessing cybersecurity risks in their programming and integrating adequate cybersecurity protections into their work, which can prevent or mitigate the effects of digital threats to democracy.[1]

1 Available USAID resources include Democratizing Digital Video and Facilitator's Guide; Digital Literacy Sectoral Briefers; Cybersecurity Sectoral Briefers.

Develop simple and practical tools to aid in identifying, measuring the severity of, and countering digital threats to democracy in educational institutions and deploying effective countermeasures.

Fund targeted research to identify how digital threats to democracy manifest in the education sector, such as the potential for digital surveillance in edtech tools or associated data privacy risks.

Design and test evaluation methods to measure the impact of digital threats to democracy and associated mitigation strategies in the education sector, with the objective of developing indicators to incorporate into activity and intervention design.

Gather evidence from USAID-funded programs on how to mitigate the impact of digital rights abuses on the education sector, in order to replicate or adapt these methods in new programming.

External-facing

Build awareness of potential digital threats to democracy in the education sector among donors, implementers, and education sector stakeholders by funding high-profile events, publications, and public communications campaigns at the national and international level.

Mitigate the risk of funding non-rights-respecting technologies in the education sector through joint investments or programs with other partners, such as multilaterals, other bilateral donors, and international organizations, in alignment with USAID's Education Policy.

Collaborate with other U.S. Government (USG) departments and agencies through interagency technical working groups to **ensure that no USG funding is allocated to non-rights-respecting edtech tools or other educational technologies**, aligned to the "One USG" approach in the USG Strategy on International Basic Education.

Facilitate the development of data governance standards, software development standards, and codes of conduct for the design and use of edtech tools and other digital services for the education sector based on the Principles for Digital Development and the principle of Do No Harm.

Recommendations for USAID Mission staff and implementing partners at the country level

These recommendations address how USAID Mission staff can raise awareness of and counter digital threats to democracy in their education sector portfolios at the country level.

Before or during project, activity, or intervention design:

- Incorporate research on these threats into country-specific education sector analyses and other analytical products such as Information and Communications Technology for Education (ICT4E) assessments to understand the potential threats to digital democracy facing the education sector in specific countries.
- Design localized programming that reflects the political context and the political economy of the education sector. To design effective programming, it may be important to examine how existing government policies restrict access to—or the development of—educational content that contradicts government influenced or directed narratives, thus limiting access to reliable and unbiased information.

- Fund hybrid online/offline education sector programs in the event of internet shutdowns. Ensure that USAID education sector programming with a digital element can work offline.
- Incorporate specific technical expertise, data, research, and proven best practices shared by other in-country USG agencies about education sector-specific digital threats to democracy into project, activity, or intervention design, in alignment with the USG Strategy on International Basic Education. This could also include co-designing interventions or co-investing in programming that aims to mitigate digital threats to democracy in the education sector.
- Conduct a data protection impact assessment and a child rights impact assessment for any edtech tools and education sector databases that USAID may fund, per UNICEF's The Case for Better Governance of Children's Data: A Manifesto.

With governments in USAID partner countries during implementation:

- Build policymaker and civil servant awareness of potential digital threats to democracy in the education sector.
- Provide technical assistance (TA) to national governments on incorporating strategies to mitigate digital threats to democracy into national level education plans, strategies, or policies.
- Provide TA to national, regional, or local governments on minimizing the collection of personally identifiable data in government-run education sector databases or other edtech tools, in keeping with USAID's effort to strengthen the capacity of partner countries in measuring and tracking learning and educational outcomes (per USAID's Education Policy).

With schools or higher education institutions (HEIs) during implementation:

- Educate and train teachers, lecturers, and administrators on how digital threats to democracy can affect their educational institutions, and how specific mitigation tactics (such as cybersecurity measures) can protect students. Build their capacity to integrate adequate cybersecurity protections into their work to help prevent or mitigate the effects of digital threats to democracy.
- Work with educational institutions to develop and implement child protection and safeguarding rules and guidelines that extend to the digital realm.[2]
- Develop context-appropriate and age-appropriate digital citizenship and information literacy curricula that cover topics including mis- and disinformation, technology-facilitated gender-based violence, online surveillance, and other digital threats to democracy to sensitize children and youth to potential digital threats to democracy.[3]
- Implement strong data protection measures to ensure that the personal information of students and educators is collected, stored, and used securely. Obtain informed consent for data collection and implement measures to prevent sensitive information from being misused or obtained by unauthorized parties.
- Identify and train moderators from individual schools and higher education institutions to monitor, identify, and contain cases of mis- and disinformation on school-related social media pages or other edtech tools.
- To combat technology-facilitated gender-based violence (TFGBV):
    - Ensure and prioritize the safety and well-being of students, especially in online learning environments, by implementing measures to prevent TFGBV, bullying, harassment, and inappropriate behavior and providing avenues for reporting concerns.

2 Toolkit: Youth Guide to End Online Gender-Based Violence | UN Women

3 FAQs: Trolling, stalking, doxing and other forms of violence against women in the digital age | UN Women

- Fund in-school counseling and other services such as support groups or dedicated online portals for students experiencing gender-based violence, including TFGBV,[4] and develop referral pathways for out-of-school support services.[5]
- Build the capacity of educators, parents, and other school or HEI employees to provide effective psychosocial support to students experiencing multiple forms of TFGBV, such as non-consensual intimate image (NCII) abuse.

With the developers of edtech tools:

- Require that edtech developers who receive USAID funds 1) apply the highest data protection and data privacy standards to students' data required by any jurisdiction that they operate in, and 2) publish their privacy policies, as well as information about how they use student data. This aligns with recommendations in UNICEF's The Case for Better Governance of Children's Data: A Manifesto.
- Upskill edtech developers on the importance of minimizing the amount of personally identifiable information that edtech tools collect about parents, students, teachers, and administrators, then work with them to modify their PII data collection processes accordingly.
- Work with edtech developers to prioritize cybersecurity by design when developing new edtech tools and to adopt the codes of conduct referred to in the previous section.

Key Trends in Digital Threats to Democracy Across the Education Sector

Digital threats to democracy such as Internet shutdowns, TFGBV, mis- and disinformation, data privacy violations, digital surveillance, and online censorship can drastically affect the ability of children and youth to acquire the skills they need for the future. These threats can have a profound impact on the education sector in USAID partner countries by undermining access to safe and secure educational technology (edtech) tools.[6] Current trends around the globe and in sub-Saharan Africa include:

- **Internet shutdowns impede access to education, and some national governments are deploying shutdowns to curb cheating on national exams**. In 2022, the United Nations' Special Rapporteur on the right to education formally acknowledged that "Internet shutdowns also often have a severe impact on the right to education, impeding learners in accessing online education, taking online exams or applying online for scholarships."[7] Mekelle University in the Tigray region of Ethiopia—subject to one the world's longest-known internet shutdowns for over two years[8]—was no longer able to use its e-learning system to teach students or provide professors with resources to conduct their research during the shutdown.[9] While all internet shutdowns impact the education sector in some way, some national governments are explicitly using internet shutdowns to curb cheating on national exams. Algeria,

4 Toolkit: Youth Guide to End Online Gender-Based Violence | UN Women; Strategies and actions for preventing and responding to technology-facilitated GBV | Social Development Direct

5 Toolkit: Youth Guide to End Online Gender-Based Violence | UN Women

6 As cited in USAID's 2021 Toolkit for Designing a Comprehensive Distance Learning Strategy, "EdTech encompasses all teaching and learning using technology in remote, in-person, and hybrid formats."

7 Impact of the digitalization of education on the right to education | United Nations General Assembly

8 Ethiopia Has Lost $410 Million To A War-Induced Internet Shutdown | Ventures

9 Impact of the Internet Shutdown in Tigray | Tghat

Ethiopia, and Sudan have all shut down their internet before and during nationwide exams.[10] These examples show that internet shutdowns impede learning among students at all levels, even when governments enact shutdowns in the name of the education sector.

- **Digital surveillance is increasing in primary and secondary schools**. Vumacam, a South African company, sells access to a nationwide network of more than 6,000 closed circuit television (CCTV) cameras and its artificial intelligence (AI) software.[11] In 2019, it launched the Kids Custodian Initiative (KCI), a pilot program that used AI to detect unusual activity in and around Johannesburg schools and to observe emergency procedures such as school evacuations.[12] This initiative raised serious questions about who had access to this highly sensitive data and for what purpose. Digital rights advocates have also raised concerns about software that monitors student activity online, although it is not used frequently in Africa. This type of software can track the specific websites visited by students, collect location data, and even allow teachers to view webcam footage of their students at home without consent.[13] Surveillance of this kind can disproportionately harm marginalized populations, with at least one school in the US outing an LGBTQI+ student to their parents based on their online search history.[14] These examples demonstrate the insidious effect of digital surveillance—both of physical schools and of students' online behavior—on the education sector.
- **Digital rights defenders and advocates for children's rights are sounding the alarm about data privacy violations in educational settings**. The use of edtech tools in schools and universities has rapidly expanded over the past several years, especially during the COVID-19 pandemic. Recent research shows that more than 90 percent of Ministries of Education around the world adopted remote learning modalities using the internet, radio, or television during the pandemic.[15] However, edtech tools generate reams of data about individual learners, and they may not have adequate privacy protections in place. Research from Strathmore University in Kenya showed that half of the 22 AI-enabled edtech platforms in its sample did not have publicly accessible privacy policies, even after registering for the platform.[16] Lack of data privacy protections is having real-world consequences for learners on the African continent: Human Rights Watch reported in April 2023 that personally identifiable information (including names, birthdays, home addresses, email addresses, photos, and passport and ID copies) of more than 70,000 Egyptian students who had taken the Egyptian Scholastic Test were exposed online for months.[17] Organizations such as UNESCO, UNICEF, and the 5Rights Foundation are increasingly exploring if and how children's right to privacy online differs from that of adults and what this means for data collected for and by educational institutions.
- **Lecturers are persecuted for posting their opinions online**. In several high-profile cases, university professors and lecturers from across the African continent have been persecuted for their Facebook posts. In March 2019, University of Hargeisa lecturer Mahmoud Jama Ahmed posted on the social media platform that people in Somalia should use established science from 'advanced societies,' not prayer, to address Somalia's drought.[18] He was convicted of blasphemy, spending nearly one year in prison until Somalia's president granted him amnesty. As a condition of his release, he was not allowed to continue lecturing or teaching for five years.[19] Prominent Ugandan activist and

10 Algeria turns off internet for high school exams | BBC; Ethiopia shut down the country's internet to beat exam Cheats | Quartz; Internet shutdowns during exams: when MENA governments fail the test | Access Now

11 South Africa's private surveillance machine is fueling a digital apartheid | MIT Technology Review

12 Vumacam's eye in the sky solution | Mail & Guardian

13 How GoGuardian Invades Student Privacy | Electronic Frontier Foundation

14 Gaggle Surveils Millions of Kids in the Name of Safety. Targeted Families Argue it's 'Not That Smart' | The 74

15 COVID-19 and School Closures | UNICEF

16 Data Privacy in Africa's Ed-Tech Platforms: Children's Right to Privacy | Center of Intellectual Property and Technology Law

17 Egypt: Data of Tens of Thousands of Students Compromised | Human Rights Watch

18 Free To Think 2020 | Scholars At Risk Network

19 Free To Think 2020 | Scholars At Risk Network

Makerere University research fellow Stella Nyanzi was arrested for cyber harassment and offensive communication in 2018 after insulting Uganda's President Yoweri Museveni and his wife on Facebook.[20] These examples indicate that online censorship and digitally-enabled targeted persecution are affecting the education sector, particularly educators at the tertiary level.

- **Mis- and disinformation is prevalent in school communities**. Children can have difficulty distinguishing between real and false information, so mis- and disinformation can cause disproportionate harm in the education sector. According to a 2022 survey of nearly 300 educators in South Africa, more than 90 percent of respondents reported that learners at their schools have shared misinformation, rumors, and false information.[21] This finding echoes research from the United States showing that more than 80 percent of surveyed middle school students could not differentiate between a real news story and sponsored content on a search engine.[22] Sub-Saharan Africa has experienced several prominent examples of mis- and disinformation touching the education sector, such as false messages on WhatsApp and Twitter accounts stating that the reopening of Grades 4 and 8 in Kenya's schools had been delayed in 2020.[23] Together, these findings indicate that mis- and disinformation are a major issue in school communities.
- **TFGBV can cause learners to leave school**. USAID's Education Policy recognizes that "Unequal power relations between adults and children and males and females contribute to this [school-related gender-based] violence, which can take place in formal and non-formal schools, on school grounds, going to and from school, in school dormitories, in cyberspace, or through cell phone technology."[24] NCII abuse (like revenge porn) has prompted women and girls to skip or drop out of school.[25] An NCII survivor from Mexico stated that after her boyfriend posted images of her to revenge porn websites, the comments prompted her to stop going to school. Universities and schools have expelled women and girls when their intimate pictures have gone public.[26] A blog post from Nigeria recounts the story of a school-aged couple whose intimate video went viral on Twitter, leading to the girl's expulsion from school.[27] These examples demonstrate that the education system is not immune to the gendered effects of digital threats to democracy and show that women and girls often experience these threats differently than men and boys.

These trends highlight the growing need for USAID and implementing partners to consciously integrate safeguarding into education sector programming involving digital tools and technology. To learn about recommendations and trends in digital threats to democracy for other USAID sectors, please refer to the following (to be linked):

- Digital Threats to Democracy - Economic Growth
- Digital Threats to Democracy - Health
- Digital Threats to Democracy - Agriculture

Please contact USAID/AFR/CPG afrdigital@usaid.gov for more information.

20 Digital Radical Rudeness: The Story of Stella Nyanzi | Center on Digital Culture and Society

21 Media literacy education in South Africa can help combat fake news - here's what's needed | The Conversation

22 Evaluating Information: The Cornerstone of Civic Online Reasoning | Stanford History Education Group

23 Beware of This Fake News Going Around Regarding Schools Reopening | Gadgets Africa

24 USAID Education Policy | United States Agency for International Development

25 Toolkit: Youth Guide to End Online Gender-Based Violence | UN Women

26 Technology-Facilitated Gender-Based Violence: An Overview | Centre for International Governance Innovation

27 Silencing Women: Nonconsensual Distribution of Intimate Images As Gender-based Violence in Nigeria (Part I) | African Feminism