Photo Credit: US Embassy Kyiv Ukraine

Digital Literacy
CONFLICT PREVENTION AND STABILIZATION

Digital Literacy and Conflict Prevention and Stabilization[1]

USAID's Bureau for Conflict Prevention and Stabilization (CPS) partners with countries affected by conflict and violence to build the foundations for peace and stability. To that end, the CPS Bureau analyzes the risks and opportunities of digital tools technologies and, if deemed appropriate in coordination with local staff and partners, will then integrate their use into programs and policy priorities.

Digital technologies can support conflict prevention and stabilization, particularly when they are responsibly used for effective public service delivery or to help information flow between citizens. In contrast to its potential as a force for empowerment and equality, digitalization has also enabled new and scaling trends of repression, manipulation, surveillance, ideological polarization, criminal or extremist expansion, gender-based violence, and the erosion of social cohesion and stability. As such, digital literacy is an increasingly critical consideration when integrating digital technologies for conflict prevention and stabilization.

Definition of Digital Literacy

USAID—building on UNESCO's definition of the term—defines digital literacy as:

> **The ability to access, manage, understand, integrate, communicate, evaluate, and create information safely and appropriately through digital devices and networked technologies for participation in economic, social, and political life.**

---

1   Unless otherwise cited, all information in this sectoral brief comes from USAID's Digital Literacy Primer. Full citation: "Digital Literacy Primer: How to Build Digital Literacy into USAID Programming" (USAID, 2022), https://www.usaid.gov/sites/default/files/documents/USAID_Digital_Literacy_Primer.pdf.

USAID's Digital Literacy Framework

To effectively and equitably achieve access, USAID's approach to digital programming must extend beyond infrastructure and devices to ensure that users possess a nuanced set of skills to meaningfully, responsibly, and safely participate in their digital ecosystem. Two pillars underpin USAID's definition of digital literacy: capacity and safety.

» **Capacity** refers to the technical knowledge and skills required to use a variety of digital devices and services such as mobile phones, tablets and computers; the internet and messaging and social media services such as WhatsApp, Twitter, and Facebook; and audio and visual tools.

DIGITAL LITERACY
The ability to access, manage, understand, integrate, communicate, evaluate, and create information safely and appropriately through digital devices and networked technologies.

CAPACITY
The technical knowledge and skills required to use a variety of digital devices and services.

SAFETY
The skills and awareness required to use digital tools carefully while navigating potential harms and cyber threats successfully.

» **Safety** refers to the skills and awareness required to use digital tools carefully while navigating potential harms and cyber threats successfully. This pillar includes, but is not limited to, strategies for strengthening cyber hygiene[2] and countering mis- and disinformation.
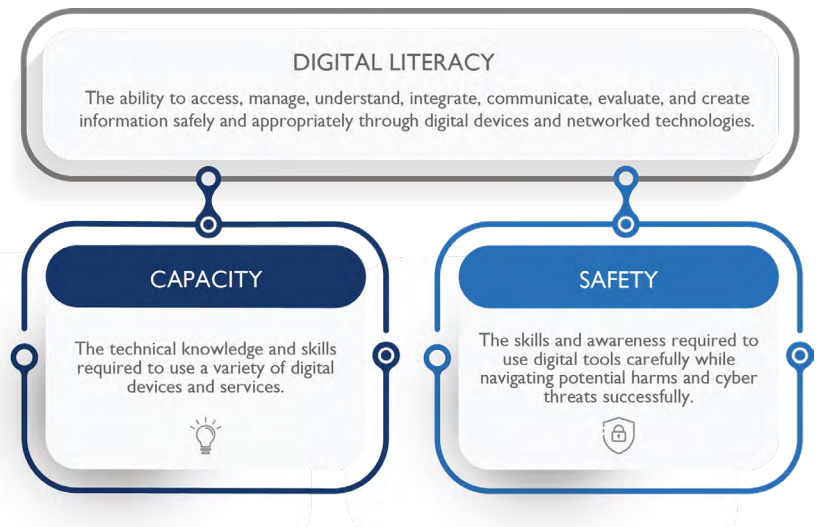
As explained in the Digital Literacy Primer, USAID takes two primary approaches to incorporating digital literacy into program design:

FOUNDATIONAL ACTIVITIES

Foundational digital literacy activities build digital literacy skills applicable to all aspects of users' economic, social, and personal lives—a goal in and of itself.

TACTICAL ACTIVITIES

Tactical digital literacy activities prepare target populations to use digital tools in particular sectors to ensure that a specific digital intervention is effective (though digital literacy may not be the singular goal of the activity).

Digital Literacy in USAID's Conflict Prevention and Stabilization Portfolio

CPS conducts tactical digital literacy activities that fill specific knowledge or skill gaps necessary to achieve higher-level outcomes in fluid, complex, and insecure environments. This work includes:

» **Strengthening intergroup cohesion.** The CPS Bureau's approach to digital literacy recognizes that secure and equitable digital development offers opportunities for groups in conflict to come together to build mutual trust, empathy, and resilient social ties and to collaborate on common goals. For example, the Center for Conflict and Violence Prevention (CVP)'s People-to-People (P2P) Reconciliation Fund program used digital skills-building activities to build bridges between Israeli and Palestinian communities in the West Bank and Gaza. P2P funds the Middle East Entrepreneurs for Tomorrow, which trained over 300 Palestinian and Israeli youth in technology and entrepreneurship—fostering deeper mutual understanding, trust, and respect and building their capacity to address cross-communal challenges.

» **Building the enabling environment for peaceful discussion and civic participation.** Digital literacy can improve the volume and diversity of public discourse and civic participation by challenging patterns of exclusion, enabling more inclusive digital approaches to peace-building, and equipping partners and beneficiaries with the tools to promote peaceful outcomes online. For example, in advance of the 2015 elections in Côte d'Ivoire, CPS partnered with Akendewa, a national civil society

---

2   Cyber Hygiene definition: The practices and steps that users of computers and other devices take to maintain system health and improve online security. These practices are often part of a routine to ensure the safety of identity and other details that could be stolen or corrupted.

Photo by New Sun Road.

organization, to train 50 young people to promote nonviolent participation in the electoral process on social media. Those young people ultimately led 20 Facebook Group discussions about the elections and also created the #civelection hashtag to share information and promote diverse conversations about the elections; the hashtag was used in more than one millions social media posts in the week of the election.

» **Mitigating risks related to hate speech and mis- and disinformation.** Though social media can serve as a tool to promote peace, it is also a vehicle for hate speech and mis- and disinformation. To counter these narratives, CPS works with partners who possess shared values around peace and democracy with the clout to influence local perceptions, attitudes, or behaviors. For example, CPS worked with university students in Ethiopia to monitor social media-based hate speech and mis- and disinformation and trained journalists on the impact of that content in the context of Ethiopia's current political and legal environment.

» **Increasing transparency and public accountability through strategic government communications and independent media.** It is critical to work with reform-minded governments who share the U.S. government's commitment to human rights and democratic values to improve their use of digital tools to communicate about the continuity of public services. Further, these governments must be able to use digital tools to respond effectively to feedback from their constituents during periods of political upheaval. It is equally important to provide emergency assistance to independent media outlets, so they can utilize digital tools in a secure manner and continue to provide access to credible, fact-checked information. For example, in late 2022, CPS began working with Lviv Media Forum, a Ukrainian NGO, to fund a new digital networking space, training opportunities, and essential media and communication equipment for journalists displaced by the Russian invasion.

» **Promoting digital hygiene and cybersecurity best practices.** Good digital hygiene and cybersecurity practices are essential, given the prevalence and weaponization of cyberattacks in conflict environments. Digital hygiene should be mainstreamed into the design, implementation, monitoring and evaluation, and risk analysis of all projects in conflict and violence-affected environments. This may involve changes to operational approaches including communication protocols, software and system consent processes, hardware or software procurement, and data management practices; further, projects can benefit from consulting with trusted and competent cybersecurity specialists who can audit the systems and processes used by USAID's partners. While working to increase media professionalism and independence and ensure greater citizen access to diverse and balanced information in the Kyrgyz Republic, the CPS Complex Crises Fund helped support local journalists to improve their defenses against cyber threats and attacks and allow them to produce content without risking software incursions.

» **Providing actionable insights on how digital tools and technologies contribute to offline and online conflict dynamics.** All of the work listed above is grounded in localized research driven by partners who have a deep understanding of the local context. This research improves local digital literacy by building a more nuanced understanding of how digital technologies contribute to offline and online conflict dynamics. For example, in Ghana, CPS worked with a multi-stakeholder team of media researchers, civil society organizations, journalists, and peace committees to better understand which narratives and digital platforms may contribute to feelings of exclusion and could be used to justify violence. This research tested assumptions on how to meet beneficiaries where they are and what motivations might be driving local exclusion and violence, and it ultimately fed into the development of projects on how to prevent conflict.

Key Considerations for Digital Literacy in USAID's Conflict Prevention and Stabilization Portfolio

Considerations vary based on the maturity level of local digital ecosystems.

☑ Employ conflict-sensitive approaches to digital literacy initiatives to mitigate the risk of doing harm and reinforcing drivers of conflict and violence. This requires deliberate effort to understand the local conflict and violence dynamics, and how these influence and are influenced by digital development.

☑ Customize digital literacy activities to specific audiences and knowledge and skill gaps. Rights, opportunities, access, and protections are experienced differently by different groups in societies. Societal exclusions and deprivations contribute to cycles of conflict and violence, and digital literacy activities should be designed with an understanding of how these dynamics affect different groups.

☑ Assess the current digital literacy gaps of the target audience to better understand which devices, platforms, and digital tools—and which of their functionalities—they use.

☑ If the target audience's digital literacy levels are highly variable, segment digital literacy interventions into different difficulty levels.

☑ Deploy tactical digital literacy training before launching or introducing any new digital tools to target users. This will help ensure that the users understand the tools' full functionalities.

☑ Assess potential risks and harms for new audiences using digital tools, and counteract them by including training on digital security, privacy, and responsible use components.

☑ Digital literacy is a recognized component of effective programs combating the myriad threats associated with hate speech and mis- and disinformation.

Photo Credit: Bluetown

☑ Assess how violent extremists are utilizing digital and media spaces to support their interests and identify concrete ways to mitigate and safeguard against these digital harms.

☑ Incorporate digital hygiene and cybersecurity skills building into all digital literacy interventions. Ensure that any digital tools provide information about how users can best protect themselves while using the tool and how their personal data will be stored and used.

☑ Sensitize implementing partners to the importance of minimizing the amount of data collected about participants in conflict-affected areas, especially personally identifiable information. Work with implementing partners to develop risk mitigation plans for data protection and management.

FOR MORE INFORMATION on the digital literacy and CPS nexus in USAID programming, please reach out to digitaldevelopment@usaid.gov or cpsdigital@usaid.gov.