



STRENGTHEN INTERNAL AND PARTNER CAPACITY FOR RISK MITIGATION AND SAFEGUARDING



Development projects and programs in a country are not, as a rule, primarily focused on digital strategies and tools; the people and partners implementing them are often not digital development experts, let alone gender and tech specialists. There is a risk that the negative consequences of women and girls using ICT could be amplified, unless individuals and organizations have clear guidelines as well as the knowledge required to implement them. It is crucial to ensure that programs are designed to consider the safeguarding of women and girls, so that they can responsibly access and use ICT.

CHECKLIST FOR ACTIONS

- ☐ Develop (or adapt) internal digital safeguarding policies, processes, and practices focusing on women and girls, that any program that has digital components must adhere to. Existing internal safeguarding principles can be adapted to include digital safeguarding principles. If a new structure needs to be created, [Girl Effect's principles](#) are a good model to follow or adapt.

What digital safeguarding processes are we developing/adapting that focus on women and girls?

HOW DOES THIS LINK TO WEEGE?

ADS 205 Domains

Access and Control

WEEGE Principles

- 1 – Understand the System
- 3 – Be Specific
- 6 – Collaborate
- 7 – Address Gender-based Violence
- 9 – Walk the Talk

- ❑ **Incorporate a digital lens into any existing GBV strategies, policies, or projects. Technology-facilitated GBV is often not integrated into broader GBV policies (including the 2016 U.S. Government GBV Strategy).**

How are we incorporating a digital lens into existing GBV strategies, policies, or projects?

- ❑ **Incorporate a technology-facilitated GBV (and wider risks) lens into any WEEGE gender analyses at the strategy, project, and activity level.**

How are we incorporating a technology-facilitated GBV (and wider risks) lens into our WEEGE gender analyses?

- ❑ **Train staff and partners on risks and mitigation strategies as well as policies to strengthen capacity; ensure that the risks are not inadvertently made worse in the implementation process.**

How are we training staff and partners on risks and mitigation strategies and policies?

- ❑ **Leverage and adapt existing training materials on risks and risk mitigation.**

How are we leveraging and adapting existing training materials?

- ❑ **Obtain buy-in from Mission Directors for leadership and sustainability.**

Which Mission Directors have we obtained buy-in from?



WEEGE IN ACTION



Photo: Paula Bronstein/Getty Images/Images of Empowerment

Online training in cybersecurity and data privacy

The Center for International Private Enterprise delivered face-to-face training workshops on best practices for digital security and data privacy for some of their partner organizations worldwide. Because it was not cost-effective to deliver only face-to-face workshops, they supplemented this with a (now publicly available) online course to reach more people, leveraging ICT and reducing cost.

DOCUMENTS IN THE GENDER DIGITAL DIVIDE RISK MITIGATION TECHNICAL NOTE



HOW TO USE THIS GENDER DIGITAL DIVIDE RISK MITIGATION TECHNICAL NOTE



UNDERSTANDING THE RISKS OF ICT TO WOMEN AND GIRLS



TOOL 1: PRACTICAL RISK MITIGATION STRATEGIES

- » **STRATEGY 1: UNDERSTAND THE CONTEXT AND THE RISKS: “FIRST, DO NO HARM”**
- » **STRATEGY 2: INVEST IN, SUPPORT, AND SHARE INSIGHTS ON DIGITAL PRODUCTS AND SERVICES THAT MITIGATE RISKS**
- » **STRATEGY 3: SUPPORT AND STRENGTHEN ICT OUTREACH AND DIGITAL LITERACY INITIATIVES**
- » **STRATEGY 4: SUPPORT INITIATIVES THAT INVOLVE (MALE/FEMALE/FAMILY) GATEKEEPERS**
- » **STRATEGY 5: RAISE AWARENESS**
- » **STRATEGY 6: COLLABORATE AND WORK WITH OTHER NATIONAL STAKEHOLDERS**
- » **STRATEGY 7: STRENGTHEN INTERNAL AND PARTNER CAPACITY FOR RISK MITIGATION AND SAFEGUARDING**



RESOURCES 1–3: KEY DOCUMENTS