DIGITAL GLOBAL CITIZENSHIP EDUCATION
FOR YOUNGSTERS AND EDUCATORS

ASSESSING DIGITAL SAFETY

01 Learning Objectives

Learners will identify risk factors in digital security and safety, and learn core principles to prevent technology-facilitated harm.

02 Connection to GCE / D-GCE / Hybrid GCE

Addresses technology-facilitated gender-based and intersectional violence in digital, hybrid, and analogue learning settings.

03 Participants

Up to 20 people (activists, educators, students, NGO staff) from diverse backgrounds.

04 Duration

90 minutes (including two polls and group reflection).

Preparation

- Set up an accessible, GDPR-compliant online space with anonymous polling.
- Gather or create slides with the 10 self-assessment statements below.
- Prepare two live polls:

1. Yes/No self-assessment (1 point per "Yes")
2. Top 3 digital-safety risks (plus "Other")

Self-Assessment Statements

01 ▶ I regularly review and update my social-media privacy settings.

02 ▶ I use end-to-end encrypted messaging apps (e.g. Signal, WhatsApp) for sensitive chats.

03 ▶ I've mapped potential digital threats based on my gender, location, ethnicity, etc.

04 ▶ I'm part of a community that practices collective digital security.

05 ▶ I feel confident teaching others about digital-safety tools.

06 ▶ I practice digital self-care (e.g. screen-time boundaries, managing online stress).

07 ▶ I use strong, unique passwords and a password manager.

08 ▶ I understand how platforms collect and use my personal data.

09 ▶ I know where to turn if I face online harassment or abuse.

10 ▶ I consider accessibility and inclusivity when choosing digital tools.

Instructions

1. Intro (10 min):

- Explain purpose, agenda, and privacy measures.

2. Poll 1 (20 min):

- Show each statement; participants answer Yes/No and tally their own score.
- Launch anonymous Poll 1; display aggregate results.

3. Reflection 1 (15 min):

Discuss which statements relate to security (data/assets) vs. safety (people/well-being) and why.

4. Poll 2 (15 min):

- Offer 3–5 common risks (e.g. doxxing, phishing, surveillance, trolling) plus “Other.”
- Participants pick top 3; share results and discuss intersections with gender and other identities.

5. Action Planning (20 min):

- In small groups, choose one top risk and design three mitigation strategies.
- Groups share back in plenary.

6. Wrap-Up (10 min):

- Summarize key takeaways and share follow-up resources.

Debrief / Reflection

- What surprised you in your self-assessment?
- How did discussing security vs. safety shift your perspective?
- Which action will you commit to this week?

Trainer Tips

- Emphasize anonymity to encourage honesty.
- Include diverse, real-world examples of intersectional harms.
- Ensure slides and polls are screen-reader friendly and captioned.
- Provide trigger warnings and referral info for support services.
- Explain that safety doesn’t always mean comfort. When others speak of injustices we haven’t personally experienced, we should resist the urge to withdraw or deny their reality. If we feel uneasy, we take responsibility by listening deeply and learning about the harms people face, especially those inflicted through digital means.
- Send a one-page “Digital Safety Checklist” after the session.

Skills – SDGs – GCE Competences

4 QUALITY EDUCATION

Self-Awareness | SDG 4: Quality Education | Learning to Learn

3 GOOD HEALTH AND WELL-BEING

Creativity | SDG 3: Good Health & Well-Being | Social Competence

5 GENDER EQUALITY

Empathy | SDG 5: Gender Equality | Civic Engagement

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE

Digital Literacy | SDG 9: Industry, Innovation & Infrastructure | Critical Thinking

17 PARTNERSHIPS FOR THE GOALS

Collaboration | SDG 17: Partnerships | Intercultural Competence

3 GOOD HEALTH AND WELL-BEING

Resilience & Self-Care | SDG 3: Good Health & Well-Being | Emotional Regulation

References & Links

- Digital-Secure Spaces List
- The Feminist Holistic Approach to Digital Security