GUIDANCE ON SAFE AND ETHICAL USE OF TECHNOLOGY TO ADDRESS GBV AND HP

United Nations Population Fund
GHRB Technical Division
Making all spaces safe

Technical Division
December 2021
What does TF GBV look like?

- Astroturfing
- Catfishing
- Cross-platform harassment
- Cyberbullying
- Cyberflashing
- Astroturfing
- Catfishing
- Cross-platform harassment
- Cyberbullying
- Cyberflashing
- Cyberstalking
- Cyberobsessional pursuit
- Deadnaming
- Deepfakes
- Defamation
- Denial of access to tech
- Denial of Service (DoS) attacks
- Documenting or broadcasting sexual assault (rape videos)
- Documenting or broadcasting sexual assault (rape videos)
- Doxing
- Electronically enabled financial abuse
- False accusations of blasphemy
- Flaming
- Gendered or sexist hate speech
- Gender-trolling
- Gender-trolling
- Hacking
- Grooming (online)
- Hashtag poisoning
- Image-based abuse
- Impersonation
- Limiting or controlling use of technology
- In-real-life (IRL) attacks
- Mobbing or dogpiling
- Online (gender) harassment
- Recruitment
- Retaliation against supporters of survivors
- Sexting and abusive sexting
- Sextortion
- Sextortion
- Synthetic sexual media
- Swatting
- Technology-facilitated unwanted sexual experiences
- Threats
- Threats
- Zoom bombing
- Zoom bombing
- Electronic enabled financial abuse
- Upskirting, creepshots and digital voyeurism
Guidance on the Safe and Ethical Use of Technology to Address Gender-based Violence and Harmful Practices: Implementation Summary
Objectives

- **Potential Benefits**: increase awareness of the potential benefits and options that tech-based interventions could bring to GBV programming;
- **Risk, Harm, Misuse**: increase understanding and reduce risks associated with GBV tech-based interventions;
- **Framework**: provide a shared framework for consistent standards and oversight;
- **Digital Intervention Process**: outline a GBV digital intervention process with considerations, steps, and tools.
Ethical stance (aka "GBV Digital Data Standards") is contextualised from the following:

- Data Privacy and Data Ethics
  - GDPR - General Data Protection Regulation
  - ODI - Data Ethics
  - IDRC/ Joint - Professional Standards for Protection Work, Managing Data and Information for Protection Outcomes (p. 103 - 148)

- WHO Research Ethics (Development, Humanitarian, Global)
  - WHO Putting Women First
  - WMA Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects

- GBV Guidance
  - Humanitarian: GBViE Minimum Standards
  - Development: VAW ESP
  - United States: VAWA - US Violence Against Women Act

Standards/ Steps and style adapted from:
- Digital Health/ mHealth
  - Planning an Information Systems Project Toolkit - Joint
  - DIIG - Joint
  - Youth-centred digital health interventions - Joint
  - WHO Recommendations on Digital Interventions
- Designing Digital Interventions for Lasting Impact - UNICEF
- Principles for Digital Development
Table of Contents

- **Definitions** – 44 tech and data definitions
- **Principles** – 6 core principles, 10 data-specific principles
- **Current Technology** – overview, specific interventions
- **Potential Benefits** – access, quality, TFGBV solutions, research, gender equality, better tech
- **Risk, Harm and Misuse**
  - Framework of Risk: Individual, Organization, Society
  - Risk by Actors: Bad, Mission-driven, and “Neutral”
- **Steps**
  - 6 Key Considerations
  - 17 Steps: Scoping, Design, Implementation, Lifetime
- **Promising Practices** – 12 promising practices
- **Annexes** – 8 stand-alone annexes
# Table of Contents

- **Definitions** – 44 tech and data definitions
- **Principles** – 6 core principles, 10 data-specific principles
- **Current Technology** – overview, specific interventions
- **Potential Benefits** – access, quality, TFGBV solutions, research, gender equality, better tech
- **Risk, Harm and Misuse**
  - Framework of Risk: Individual, Organization, Society
  - Risk by Actors: Bad, Mission-driven, and “Neutral”
- **Steps**
  - 6 Key Considerations
  - 17 Steps: Scoping, Design, Implementation, Lifetime
- **Promising Practices** – 12 promising practices
- **Annexes** – 8 stand-alone annexes
Core Principles:
- Do No Harm
- Survivor-centred
- Informed Consent and Transparency
- Participatory
- Rights-based
- Advancing Gender Equality

Data Specific Principles:
- Safety by Design
- Purpose limitation
- Data minimization
- Proper use of data
- Fairness
- Informed Consent, Transparency, and Ownership[
- Accuracy and Data Quality
- Security: Integrity, Confidentiality, and Availability
- Accountability
- Unconditional service

Potential Benefits

- Amplifying positive social norms
- Facilitating delivery and improving the quality of services
- Increasing access to information & services
- Increasing gender equality and closing the gender digital divide
- Facilitating research, and increasing robust evidence, findings and insights
- Combating technology-facilitated GBV
- Increasing our future ability to create better tech for GBV

*List not comprehensive*
RISKS & HARMS - Framework of Risk

Society
Gender Inequality Amplified

Organization, Group, Community
Reputation
decreased confidence in safe service delivery

Individual:
Survivor, Responder, Advocate, Staff, Affiliate
Death, GBV, including TF GBV

Note: GBV = gender-based violence; TF GBV = technology-facilitated gender-based violence

UNFPA [2023]. Guidance on the Safe and Ethical Use of Technology to Address Gender-based Violence and Harmful Practices: Implementation Summary
RISKS & HARMS - Threat Actor Mapping

Perpetrators: Intimate Partners, Family Members, Strangers, Friends, Acquaintances

Financially Motivated Hackers or Opportunists

Governments or Politically Motivated Groups (targeting empowered women)

Misogynistic Individuals or Groups

RISKS & HARMS – Type of Actors

MALICIOUS
Conscious decision to act inappropriately
Motive to harm

NEGLECTED
No conscious decision to act inappropriately

ACCIDENTAL
No motive to harm

Safety, privacy and security are a three-legged stool.

What happens if one leg is missing or breaks?

The stool will fall over!

Embed privacy into the design specifications of information technologies, organizational practices, and networked system architectures in order to achieve the strongest protection possible.

Establishes user safety at the center of product development, recognizing the potential risks and harms in the online spaces. Details 3 overarching principles: (1) service provider responsibility (2) user empowerment (3) transparency and accountability.

Design controls to prevent the misuse of an application by malicious parties. A proactive, necessary process of planning, monitoring, and adapting to changing cyber threats.
Considerations and Steps

**Considerations:**
- Do No Harm
- User Integration/ Participatory
- Use and Accessibility
- Safeguarding/ Managing Risk
- Data Analysis
- Consent

**Steps**

**Scoping/ Feasibility**
- STEP 1: Risk-Benefit Analysis
- STEP 2: Lifetime Cost

**Design**
- STEP 3: Needs, Purpose, Outcome
- STEP 4: Research
- STEP 5: User Integration
- STEP 6: Confirm Data Privacy Principles
- STEP 7: Ideation
- STEP 8: Prototype OR Select/ Adapt Solution
- STEP 9: Systematic User and Product Testing
- STEP 10: Budget creation/ adjustment
- STEP 11: Consent Check
- STEP 12: Content Alignment with Global Standards Check
- STEP 13: Build
- STEP 14: Safety, Security, and Privacy Check
- STEP 15: Live Pilot Test
- STEP 16: Adjust/ Fix

**Implementation**
- STEP 17: Implementation

**Lifetime**

Considerations and Steps

Considerations:
- Do No Harm
- User Integration/ Participatory
- Use and Accessibility
- Safeguarding/ Managing Risk
- Data Analysis
- Consent

Steps

Scoping/ Feasibility
- STEP 1: Risk-Benefit Analysis
- STEP 2: Lifetime Cost

Design
- STEP 3: Needs, Purpose, Outcome
- STEP 4: Research
- STEP 5: User Integration
- STEP 6: Confirm Data Privacy Principles
- STEP 7: Ideation
- STEP 8: Prototype OR Select/ Adapt Solution
- STEP 9: Systematic User and Product Testing
- STEP 10: Budget creation/ adjustment
- STEP 11: Consent Check
- STEP 12: Content Alignment with Global Standards Check
- STEP 13: Build
- STEP 14: Safety, Security, and Privacy Check
- STEP 15: Live Pilot Test
- STEP 16: Adjust/ Fix

Implementation
- STEP 17: Implementation

Lifetime


Understand and design for the context and users’ actual needs.

Adopt human-centred and participatory approaches to design.

Plan data analysis and data use from beginning.

Use research-backed and evidence-based approaches.

Bake informed consent into the entire intervention.

Iteratively test and learn with users.

Monitor and evaluate success, challenges, and safety concerns.

Sustainability – clear view beyond product launch.

Alignment with GBV national priorities and global standards.

Build strong interdisciplinary development team (IT, Digital, GBV, women’s organisations).

Consider open-source and modular approaches when safe and appropriate.
Annexes

- **Annex A: Risk Benefit Analysis Tool**
  - Risk Factors – Data Security and Indicators of Heightened Risk
  - Assessing Harm – Rights, Economic, Psychological, Social
  - Benefits – Impact, Likelihood, Outcomes for Survivors

- **Annex B: GBV Digital Essentials: Dos and Don’ts**
  - Harms and Risks, Understanding Users, Consent, Safety, Security, Digital Ecosystem, Collaboration, Lifetime

- **Annex C: Checklist: Essential Considerations**
  - Scoping/ Design/ Launch/ Lifetime

- **Annex D: In-House vs. Cloud: Pros and Cons**

- **Annex E: What to Consider in a Partnership**
  - Selecting the right vendor

- **Annex F: Contingency Planning: Priorities in an Emergency**

- **Annex G: Data Mapping Workshop Template**

- **Annex H: Data Myths, Facts, and FAQs**