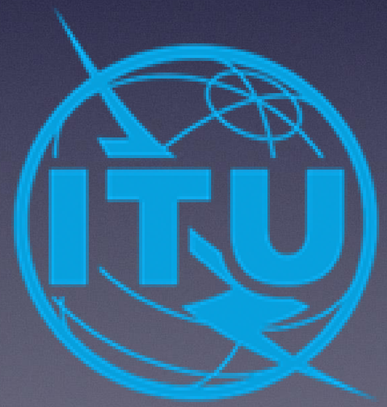
Guidelines for Industry



Five Key Areas for Industry

1. Integrating child rights concerns into all appropriate corporate policies and management processes
2. Developing standard processes to handle child sexual abuse material (CSAM)
3. Creating a safer and age-appropriate online environment
4. Educating children, carers, and educators about children’s safety and the responsible use of ICTs
5. Promoting digital technology as a mode for increasing civic engagement

General Guidelines

Integrating Child Rights Concerns Into all Appropriate Corporate Policies and Management Processes

Integrating Child Rights

- Called for by UN Guiding Principles on Business and Human Rights
- Privacy and freedom of expression especially important to protect
- Comply with national regulations, and preferably meet or exceed international standards
- Take care to avoid unintentional compromise of child’s rights

Develop a Child Protection Policy

- Establish a Child Protection Policy Management team with oversight and authority on COP
- Consult with stakeholders (including children) on how best to empower and protect rights of children
- Ensure policy meets or exceeds international standards
- COP due diligence: Evaluate whether company may be contributing to adverse effects on children

Features and Evaluation

- Grievance reporting system
- Age-appropriate design
- Automated screening for inappropriate activity and content
- Break down impact assessments by subgroup, such as age

Developing Standard Processes to Handle CSAM

Child Sexual Abuse Material

- Widespread problem: Internet Watch Foundation found >100,000 sites with it in 2019
- Extensive eradication efforts from governments and nonprofits, but industry has a role too

Reporting CSAM

- Have reporting service
- Publicize hotlines for CSAM reporting: law enforcement, child safety nonprofits (e.g IWF, ICMEC — INHOPE has extensive list)
- Forward reports to law enforcement and international child safety organizations
- Ensure process minimizes exposure of persons to material and provide support for staff’s mental health

Handling CSAM

- Create team to integrate CSAM-fighting efforts into the product and report on progress
- Block reported material but do not delete until instructed to
- Cooperate with law enforcement
- Create data retention system to assist investigations
- Document all staff who have handled CSAM as part of their work

Technological Tools

- PhotoDNA: Privacy-preserving photo and video scanning from Microsoft
- Project Artemis: Analyzes chats to find signs of grooming, also from Microsoft
- IWF has CSAM detection and blocking tools, and lists of domain names for ISPs
- Regularly use these tools to scan for CSAM

Creating a Safer and Age-Appropriate Online Environment

Reducing Risk

- Recap: Risks are content, contact, and conduct, and may be aggressive, sexual, values-based, or commercial in subject
- Risk won’t be eliminated, but can be reduced
- Children’s agency creates risky behavior, which helps develop autonomy and resilience
- Where risk is still significant, users can be informed
- ICT aimed at children is held to a higher standard

Open Communication

- Communicate professionally and clearly with children
- When material may be inappropriate for children (e.g. user-generated content), indicate that beforehand
- Be transparent about how parental controls impinge on child privacy rights
- Provide clarity on what products or services are available
- Indicate target age group, possibly using local content rating systems

Positive Environment

- Use a code of conduct to indicate behavioral expectations
- Moderate social spaces to prevent harassment, impersonation, etc.
- Make avenues of reporting clear
- Handle reports in a timely fashion and allow an appeal
- Communicate with reporter and subject of report about status of report

Privacy and Content Controls

- Minimize data collection from children, following privacy-by-design
- Use privacy-preserving technologies where possible
- Consider providing parental control tools, including purchase and time limitations
- Consider age verification to steer children to age-appropriate spaces
    - Be cautious of constraining their freedom of expression or violating their privacy

Industry Interactions

- Hire carefully for people who work with children
- Ensure advertising is child-safe
  - Advertised products shouldn’t be harmful to children
- Collaborate with other businesses to share COP insights

Educating Children, Carers, and Educators About Children's Safety and the Responsible Use of ICTs

The Role of Industry in Education

- Awareness raising and education vital
- Responsibility shared with schools and parents
- May be most effective working indirectly
  - Parents and teachers know child’s circumstances better, but may need education themselves

Education Topics

- Promote respect of age limits
- Show parents how to help their children use the service
- Highlight and provide clear instruction on parental controls and safety features
- Use plain language that’s locally comprehensible

Partnerships

- Engage with stakeholders to find the best ways of educating
  - Government, educators, parents, children, other businesses
- Child online safety nonprofits can provide valuable guidance

Child Online Safety Guides

- Digiworld: Game and associated educational material from Telenor
- Be Internet Awesome + Interland: Curriculum and game from Google
- Telefónica and Capital Humano y Social Alternativo’s virtual courses
- Twitter’s media literacy campaign
- Project deSHAME: Toolkit and resources on sexual harassment for schools and law enforcement from Facebook and the EU

Promoting Digital Technology as a Mode for Increasing Civic Engagement

“The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child’s choice.”

–Article 13 of the UN Convention on the Rights of the Child

Civic Participation

- Industry can actively facilitate youth civic participation
- Ensure that efforts to protect children don’t stifle their right to participate and express themselves
- Close digital divide so all voices are heard

Avoiding Silencing

- Codify right to participate in policies
- Careful that channeling children to environments aimed at them doesn’t sequester them where adults won’t hear their voice
- Don't over-block material
  - Can hinder engagement and development of resilience
  - Make clear when material is blocked
  - Allow blocking to be appealed

Empowering Participation

- Develop platforms for youth civic expression
- Inculcate creative thinking and problem solving in users
- Promote digital literacy and ICT skills
- Expand access to underserved populations

Feature-Specific Guidelines

Special Focus Industries

- Digital Infrastructure
- Media and Gaming
- Social Media
- Artificial Intelligence

Digital Infrastructure

About Digital Infrastructure

- Examples:
  - Connectivity providers/ISPs
  - Hosting services
  - Data storage providers
  - Internet cafes
- Not as visible to children as other ICT companies
- Often very large, but as small as a shop with an open WiFi router

Fighting CSAM

- Collaborate closely with government and law enforcement
  - Provide ICT education to law enforcement agents
- Use blocklists, such as from IWF, to prevent access to CSAM domains
- Enable user reports, instructing on what is illegal and how to report
- Have a procedure for complying with takedown notices

Building a Safer Environment

- Create blocking and filtering tools
  - Alternatively, highlight existing ones
- Public WiFi providers should consider filtering content, especially if children will access the network, and encrypting network traffic
- Hosting services should have abuse-reporting features

Media and Gaming

About Media and Gaming

- These offer selected and designed material
  - Websites that create their own content, such as news sites
  - Games
  - Video and multimedia services

Building a Safer Environment

- Use a content rating system that’s consistent through the industry
- Clearly distinguish advertising from content, and regulate advertising to children
- Use age verification to restrict content aimed at an older audience
- Stick to either material aimed at children or at adults

Education and More

- Encourage parental involvement in child’s consumption of media
- Combat addictive behavior, particularly for gaming providers
- Only include images of or information about specific children in material with good reason
- Detect, hide, preserve, and report user-generated content containing CSAM
- Develop age-appropriate material aimed at kindling civic interest in youths

Social Media

About Social Media

- Categories:
    1. Messaging apps (e.g. WhatsApp, Telegram)
    2. Social networking and content discovery services (e.g. Facebook, TikTok)
    3. Livestreaming services (e.g. Twitch, YouTube Live)
- Some in-between, such as Snapchat (1&2) or OnlyFans (2&3)

Building a Safer Environment

- Have stricter default privacy and content-sharing settings for younger users
- Ensure users have tools to block and report unwanted communications
- Consider restrictions on access to discussion groups with content inappropriate for younger users
- Incorporate children’s perspective into developing content moderation scheme
- Remove shared content containing children’s sensitive personal information

Education and Fighting CSAM

- Create a formal reputation system to encourage positive behavior
- Obtain permission of children appearing in featured user-generated content
- Proactively scan user-generated content for CSAM as it’s uploaded
- Inform users that illegal material, including CSAM, will be taken down and may result in banning or legal action

Artificial Intelligence Systems

About AI

- Sometimes referred to as “machine learning”, “deep learning”, etc. — a somewhat hazy domain
- Growing in prevalence, capability, and range of application
  - Facebook uses an automated system to detect material promoting self-harm
  - Instagram uses one to find cyberbullying
- But programs do exactly what you tell them to do, not what you mean!
  - E.g. drive engagement by directing children to extreme content

Building a Safer Environment

- AI systems should ideally provide transparency and explanations of decisions they make
  - Where possible, decisions should have human oversight, or at minimum be possible to appeal to human adjudicators
- Have means of recourse in case of possible harm by AI systems
- Be careful in using real child data to train an AI system: seek permission and do not make users take part
  - However, a system trained without a diversity of data may be inaccurate

Child Rights and More

- Child-facing AI should be designed for a purpose aligned with the Convention on the Rights of the Child
- Work to develop policies integrating AI ethics and child rights
- Consider ways AI systems can advance children’s education