

2023 GLOBAL OPEN CALL FOR PROPOSALS

Investment Pillar B: Research and Data

TECHNICAL NOTE

See the Full Call for Proposals Document for Application Details & Requirements across all Investment Pillars.

- **Geographical targeting:** Global
- **Grant duration:** Maximum 2 years
- **Proposal budget:**
 - Non-profits (Research & Data): up to USD 250K
 - For-profits (all Safe Online pillars): up to USD 250K
- **Eligible organisations:** Non-profit organisations, such as civil society organisations (CSOs), non-governmental organisations (NGOs), international organisations, research and academic institutions; For-profit organisations (private companies). Consortia of organisations with different strengths and expertise are highly encouraged.
- **Deadline for applications:** 31 October 2023 11:59PM EST
- **Submit proposal at:** [Online Form](#)

If you have any questions about the Request for Proposals, do not hesitate to contact the Safe Online team. Please submit questions through this [FORM](#). Answers to all questions submitted will be shared publicly.

Research and Data Additional Details

There is an urgent need to generate evidence to build a more comprehensive understanding of the threats of digital harms to children, including some of the worst forms such as online child sexual exploitation and abuse, at national, regional and global levels. The existing gaps and fragmentation of data is partly due to ethical and methodological challenges to measure abuse, cost and time to conduct national prevalence surveys, socio-cultural taboos related to sexuality, lack of reporting due to limited adequate support services, low investments from governments, lack of transparency of industry data, no clarity of how different data sources talk to each other, and an inconsistent and unclear understanding of how child sexual abuse manifests in digital environments. The lack of systematic and harmonised data collection and infrastructure for robust analysis of online risks and harms for children in the context of other forms of violence and across levels remains a critical barrier to securing a safe internet for children. These gaps impact the accurate identification of problems and needs, and the effective measurement of progress. They also undermine investments and advocacy resulting in limited political attention and financial resources allocated to the issue.

We will seek to fund academic and/or applied research or data initiatives which may draw from a range of quantitative, qualitative or mixed methods. Evidence generation efforts should increase understanding across three specific areas of interventions of online CSEA and related forms of harms to children:

1. **Prevention and deterrence of harm.** To prevent harm to children we must identify ways to promote safety in digital environments and put in place deterrence measures that identify and disrupt risky situations before harm happens. Innovative education interventions beyond PSAs and research efforts more broadly are critical pieces of prevention work. We will seek to fund research that includes but is not limited to evidence generation to:
 - o Understand how children use safety tools, compare how they do or do not report across geographies, and highlight cultural differences using the same tools/educational materials through better assessment of education initiatives, outreach strategies, or product design features in platforms.
 - o Understand motivations/ drivers/precursors for i) perceived first person CSAM, ii) non-consensual sharing of CSAM, iii) distribution, consumption or direct involvement in online CSEA.
 - o Understand motivations/ drivers/ precursors for help-seeking behaviours of i) victims, ii) offenders/potential offenders.
 - o Identification of early warning signals and applications to tools and policies to improve harm reduction techniques for behaviours such as i) offending, ii) peer to peer sharing of CSAM by minors, iii) non-consensual sharing of CSAM iv) grooming.
 - o Strengthen interventions in new technology platforms and digital environments such as livestreaming, ‘metaverse style’ communities, or AR/VR environments through better understanding of i) children’s experiences of harm online, ii) pathways of offenders into perpetration of harm.

Ex am ple s	Academic	Applied
	- Assess psychological drivers of behaviours and impacts of differential messaging on help seeking/ reporting/ deterrence; across languages and social cultural contexts. - Generate data on how online child sexual exploitation and abuse manifests in different country contexts or for different population groups, particularly those facing multiple risk factors such as children with disabilities, children in conflict or humanitarian settings, LGBTI+ youth, etc.	- Measure effectiveness of education initiatives, deterrence messaging, or product design features in platforms for i) reporting instead of resharing by the public of child sexual abuse material (CSAM), ii) peer to peer sharing of nudes by minors. - Tools and strategies for product development considerations such as safety-by-design, age-appropriate design and experiences, and mitigation of "algorithmic harm" (e.g. recommendation engines being leveraged for abuse, or unintentionally linking offenders/potential offenders together).

2. **Detection and reporting of harm.** Advancements in technology must both be leveraged to quickly and accurately identify and act on digital harm such as online CSEA as well as be better understood to disrupt potential new harms bad actors can exploit them for. This includes for example detecting CSAM within new technological environments as well as increasing the ability to detect complex interactions like grooming or solicitation. Alongside technological measures, effective reporting (by or on behalf of children) both to and by trusted adults, hotline and helplines, and technology companies is a crucial tool in identifying

online abuse and exploitation and as well as identifying offenders. We will seek to fund efforts that identify and explore expanding research and data on topics such as:

- o Effective tools and strategies for promoting reporting such as including culturally responsive and developmentally appropriate resources.
- o Landscape analysis or evaluation of best practices for technology tools and interventions.
- o Implications of evolving technology such as: i) abuse detection in encrypted or AR/VR environments, real-time detection and reporting in livestreams, implications of generative AI / synthetic data or imagery; ii) considerations of the intersection of privacy and children's rights such as policy/legislation related to tech industry practice, data protection, etc; iii) consequences for changes in offender or children's behaviour.
- o Understanding differential children's experiences in digital environments and psychological and behavioural impacts of abuse such as: i) how abuse changes children's experiences of using digital platforms, ii) what they avoid, iii) where they are comfortable online considering general social interactions to minimise digital exclusion as an additional harm.
- o Implications and impacts on users of legal frameworks for privacy / safety considerations such as approaches to (de)criminalisation of various content or behaviours (e.g. sharing of perceived first person CSAM, self-reporting, help-seeking for potential offenders etc.).

Ex am ple s	Academic	Applied
	• Investigation and mapping of common challenges or reasons for lack of reporting or data across geographies and technologies/platforms (i.e. Global South countries; immersive or distributed technologies or startup/SME/alt-tech platforms). • Understanding of commoditisation of access to CSAM, such as gaming platforms or profitability of paywalled CSAM.	• Best practices for technology tools and interventions such as false positive (and false negative) reduction techniques (e.g. PhotoDNA, ML classifiers) or racial/ethnic/cultural/gender/geographic diversity for labelling and annotating for content moderation and review of suspected CSAM.

3. **Response and support to the full ecosystem, especially victims.** Coordinated, collective response is necessary to maximise impact of interventions. Support systems and resources need to be accessible to victims in their differential experiences of online CSEA, children and families in navigating digital environments, professionals working with children's digital safety (e.g. content moderators, law enforcement, direct service providers, etc.), as well as potential and actual offenders. We will seek to fund research that increases:

- o Understanding of user experiences during and after reporting for provision of meaningful, accessible resources and platform affordances for victims and survivors based in differential experiences (i.e. racial/ethnic/cultural/gender/geographic).
- o Tailored support and response for impacts of abuse in different digital environments (e.g. across different platforms) or physical environments such as

abuse carried out by those in the family circle, those known to the individual, unknown entities, or when CSAM is self-produced content.

- o Integrated analysis of the entire cycle of online abuse – online abuse, online report, online response and support, deployment of offline reporting, offline protection services – to better understand gaps and connections to offline support systems for different ages / population groups of children as well as for families or (potential) offenders, taking into account quality and capacity of support services, timeliness, language and culturally-competent care.
- o Evidence base for actionable reporting by public, industry platforms or trusted flaggers.
- o Evidence base for effective investigation by the appropriate authorities including better understanding of reporting outcomes and improved feedback loops with law enforcement.
- o Interventions for improving trauma-informed approaches to well-being and resilience for staff such as content moderators and others.
- o Improved efficacy of support services (e.g. human such as vetted service providers or automated such AI chatbots) and understanding of differential experiences in interactions for children, victims and survivors, parents and caregivers, offenders, etc.
- o Mechanisms or infrastructure for data sharing, data governance and responsible data use, including best practices on how to make data insights accessible and digestible for different audiences in order to enable effective data use.

Ex am ple s	Academic	Applied
	• Differential experiences of children and young people around responses to reports of self-produced content and peer-to-peer abuse. • Trauma-informed approaches to support for professionals working with exposure to CSAM.	• Tools and strategies for cross-sector collaboration such as knowledge exchange around signals, suspicious behaviours, best practice and/or cross-platform reporting, data sharing, cross-analysis (e.g. extent of cross-platform interactions to identify nudges and friction surfaces.)

Scoring and mandatory criteria

All received proposals will be scored according to the following criteria:

MANDATORY CRITERIA

Criteria	Specific Criteria	Score
1. Legal registration	Registered as a legal entity (nonprofit or for-profit organisation) in the country or countries of implementation. In addition to this, letters of support from local authorities and organisations may also be required.	Yes/No
2. Alignment with priority objectives, modalities and areas	The proposed solution addresses one or more of the main objectives, modalities and areas set in this Call.	Yes/No

3. Safeguarding	The entity has a Safeguarding Policy and procedures in place (including data privacy) or is willing to develop a policy.	Yes/N o
4. Track record of implementation (only for the Investment Pillar A: "Networks and Systems")	Track record implementing similar projects in similar contexts (at least 3 project references with the corresponding supporting documentation shall be provided). For transnational projects, track record of success delivering activities to tackle online CSEA regionally and internationally (at least 3 projects).	Yes/N o
5. Organisational capacity and references	Your organisation shall be able to provide auditing records or a micro-assessment. ¹	Yes/N o

SCORING CRITERIA | Research and Data

Criteria	Specific Criteria	Score
1. Relevance & novelty of the research	- Alignment between need/gap identified and research questions proposed - Add value and/or address gaps in the existing child online safety ecosystem, does not duplicate, and/or builds upon and/or interacts with existing research and data - Generating innovative actionable or exploratory research by: - Developing new research; - Expanding existing research; or - Developing a new application / use case of existing research. - Proposals should be representative and inclusive, including countries of applicants, key partners, and population focus.	25 Points
2. Likelihood of impact and feasibility	- Overall probability of successful delivery of the research and the chance that the predicted impact and insights will be realized. - Gender equality, disability and social inclusion (GEDSI) principles incorporated in the design and implementation of the project as applicable. - Ensuring feasibility of the research and outputs - Robust design, methodology and outputs described. - Required data access in place including any necessary agreements. - The proposed research complies with existing and relevant regulatory and ethical frameworks. - Ensuring actionability of the research - Considering uptake and translation to applications of research outputs. - Producing open access research and outputs to the extent possible. - A clear Theory of Change and Results Framework is included.	25 Points

¹ If your organisation does not have this readily available, a description of why audits are not available and further financial documentation will be requested for the required due diligence.

3.Scope and inclusivity of the research	- Representation of traditionally underrepresented groups in the research (BIPOC15, LGBTQI+16, children out of school, children living in poverty, children with special education needs and disabilities, and those with relevant lived experience including survivors of online CSEA) and age and gender-disaggregation, i.e. sex and/or gender analysis, are taken into account in the research and may have different experiences with platforms - Describe considerations of cross-cultural and context-specific approaches. - Integration of children's views and child-rights centred approaches in the program and activities design. - Intersection between technology facilitated abuse, and other forms of violence against children, ensuring it articulates how it addresses other forms of violence and multiple risk factors.	20 Points
4. Suitability of the team and partners to implement the research	- Alignment of team members' proficiency and experience with skills and time commitment needed to implement project. - Team is diverse. We encourage gender diversity and representation from diverse contexts, countries and cultures as well as applications with representation from or inclusion of Global South countries, underrepresented populations such as BIPOC10, LGBTQI+11, people with disabilities, and those with relevant lived experience including survivors of online CSEA. - Team is primarily composed of individuals with direct local knowledge and connections to the country where the solution is being built and piloted. - Existence of relevant partners. - Existence of consortia with different type of organisations. - We encourage the inclusion of relevant advisers and partners to fill team's expertise gaps, as well as the formation of consortia with different type of organisations.	20 Points
5. Budget and Value for Money	- We require alignment of project activities with team capacity and budget allocation for most effective and impactful use of resources. - We seek applications with availability to match the funding. - We encourage allocations for travel to key outreach and dissemination events related to the research project.	10 Points
TOTAL SCORE		100 Points

Checklist for submission:

- Full proposal form (via Jotform online)
- Annex 2- Results Framework and Project Milestones and Implementation Plan (as per Safe Online template)
- Annex 3- Budget and Financial Reporting Template (as per Safe Online template)
- Annex 4.b.1- Evidence of research / methodological experience (as per your own template or directly as links/uploads in the Application form) (Applicable only for the Investment Pillar B: Research and Data pillar)

- Annex 4.b.2- Compliance (as per your own template or directly as text/links/uploads in the Application form) (Applicable only for the Investment Pillar B: Research and Data pillar)
- Annex 5- Sub-contracting form (as per Safe Online template) (Not applicable to UNICEF applicants)
- CVs of the team (as per your own template)
- Safeguarding policy (if the applicant has one) (as per your own template)
- Audit reports or micro-assessment (as per your own template)