2021 OPEN CALL FOR PROPOSALS

Technology solutions to make the internet safe for children

INFORMATION, INSTRUCTIONS, AND GUIDELINES

Focus: Technology Solutions to Make Digital Spaces Safe for Children

Geographical targeting: Global

Maximum funding proposal: Up to US$ 750,000 per proposal for non-profit organizations and up to US$250,000 per proposals for private companies

Project duration: Maximum 2 years

Deadline for applications: 15 November 2021, 11:59 PM EST

Submit proposal at: Apply here

Index

1. Summary

Since 2016, through its Safe Online initiative the Global Partnership to End Violence against Children has invested US$48 million in 60 projects with impact on over 70 countries. This call is focused on **solutions that leverage existing and new technologies to prevent and combat online child sexual exploitation and abuse (CSEA)**, following the 2020 Call also focused on Technology Solutions to keep children safe online.

End Violence Safe Online initiative will be looking into scaling/adapting existing and developing new technologies, such as artificial intelligence, machine learning, augmented reality, virtual reality, Internet of Things, blockchain, and other innovative solutions that have the potential to enhance prevention, detection and response to online CSEA in a rights-aware manner that supports multiple stakeholder perspectives and involves children and young people in their design and development.

Funding is not necessarily limited to the above. We are interested in solutions that apply technology in novel, ground-breaking ways that are scalable and globally applicable, enhancing the capacity of all stakeholders to address online CSEA and make children safe online.

We are looking for solutions that can help **achieve one or more of the four specific objectives below:**

1. **Detect, remove and report images and videos** with sexual content involving children and adolescents (often referred to as child sexual abuse material, or CSAM) in a way that is effective for taking action for victim assistance and prosecution.
2. **Block adults' exploitative/inappropriate access to children on digital platforms** intended to sexually abuse them (*usually referred to as online sexual grooming or solicitation*)
3. **Stop live streaming of child sexual abuse** performed in front of a camera (*usually referred to as live streaming of CSEA*).
4. **Prevent online sexual abuse of children before it happens**, including prevention of non-consensual sharing of explicit images of children, and prevention and deterrence solutions that directly target the online child sexual offenders and adults with a sexual interest in children.

The Safe Online initiative has a clear preference for proposals that can demonstrate:

- active **involvement of local partners and authorities** in the design and delivery of activities including strengthening of local capacity through the project;
- a **cross-sectorial and holistic approach** including the interlinkages between online violence and other forms of abuse against children;
- **strategic partnerships** with the Safe Online grantees and partners across levels;
- **alignment with other End Violence initiatives** such as Pathfinding Countries and Safe to Learn; and,
- availability to match the funding, and a strong evaluation and impact assessment component.

Who can apply? For this open call we are actively seeking submissions of proposals from non-profit, such as civil society organisations (CSOs), non-governmental organisations (NGOs), international organisations, research institutes and academic institutions. For-profit organisations, such as private companies, are also eligible to apply. Consortia of organizations with different strengths and expertise are highly encouraged. Please refer to section III for greater details on the eligibility criteria.

Funding modalities

The 2021 Online Open Call for technology solutions will be available through two modalities: (A) project grants and (B) equity-free investments. See the summary of the funding modalities and available funding in the table below:

Funding modality	Who can apply	Max duration	Allocation amount
A. Project grants	Not-for-profit organisations and private companies	2 years	Up to US$ 750,000
B. Equity-free investments	For-profit organisations, such as private companies	2 years	Up to US$ 250,000

How to apply? Proposal applications must be submitted through the End Violence Safe Online 2021 Open Calls Webpage, where you will also find all the relevant information and annexes for your proposal. All submissions must be made in English, please refer to the Full Proposal Application Pack.

The last day for submissions of applications is **15 November 2021 11:59 PM EST**. Only shortlisted applicants will be contacted and may be requested to provide additional clarification, as applicable.

If you have any questions about the Request for Proposals, do not hesitate to contact the Safe Online team. Please submit questions through this FAQ Form. Answers to all questions submitted will be shared publicly.

You can find further information on Online CSEA and End Violence's response in Annexes 1 and 2.

2. General conditions

We are actively seeking submissions of proposals from:

- **not-for-profit organisations**, such as civil society organisations (CSOs), non-governmental organisations (NGOs), international organisations, research institutes and academic institutions, for the grant portion of this funding; and
- **for-profit organizations**, such as private tech companies working on solutions for the prevention of online CSEA, for our equity-free investments.

Consortia are also encouraged to apply, however, the organisation submitting the application will be considered the main grantee, bearing all the contractual responsibilities vis-à-vis End Violence.

Please note that most of the available funds under this Open Call aim to support projects which will benefit countries eligible for ODA support. A small portion of the funds is not subject to this restriction.

Review and award process

End Violence awards grants through an open, fair and competitive process. All proposals will be assessed on their overall quality with attention paid where applicants have clearly explained the contextual challenges, the specific and measurable results that they expect to deliver, the strategies to achieve them with a focus on tailored approaches and interventions. In addition, applications are expected to acknowledge any risks to delivery and demonstrate plans to mitigate as such.

Organisations are asked to list partners and advisors. We encourage maximising synergies across jurisdictions/ sectors/ communities, as well as awareness of and sharing with existing projects. Funded projects will be connected to similar projects in other countries, which should enable projects to develop faster and better. More information about the Safe Online portfolio of grantees is available on the End Violence Partnership website.

End Violence Safe Online's initiative encourages and will give preference to projects that are open access. It also aspires to have any research or outputs that it invests in made available to the widest range of actors possible.

Under this Call, eligible proposals may result in signing of a Grant Confirmation Letter for a period of up to two years and up to US$ 750,000 or US$ 250,000 (depending on the funding modality). Considerations of proposals that require more funding than the indicated amount will be considered by End Violence at its sole discretion and only if this is in the best interests of achieving the goals of the funding round. In addition to the relevant costs for the implementation of their project, applicants are strongly encouraged to make provisions for evaluation of their projects (10-15% of the total direct costs) and contingencies (i.e. fluctuations of exchange rates and unforeseeable circumstances, up to 5% of the total direct costs).

Most significantly, proposals will be evaluated for alignment of the scope and activities outlined with the proposed budget. Payment will be made to the applicant's institution, and in the case of a consortium, to the main grantee organisation. Grantees' instalments are determined based on their proposed budgets, with 1-2 instalments depending on project duration and budget. Indirect costs are limited to 7% for grants.

Please note that if you are selected for a Grant award, your organisation will be asked to submit two years of the latest financial audit reports. 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 by End Violence. As End Violence is hosted administratively by UNICEF, organisations without a risk rating within UNICEF's financial management system may be required to undergo a financial micro-assessment during the grant period.

End Violence's Safe Online initiative will actively monitor the progress of all supported projects during the period of the grant, and periodic evaluation of progress. Specifically, all grantees will be required to:

- Report on project progress during annual reporting periods using the Safe Online's reporting templates, which will be provided to grantees;
- Establish and report on key milestones according to qualitative and quantitative indicators selected by the grantee based on their project proposal using Safe Online's Monitoring & Evaluation template which includes suggested indicators;
- Report on key potential barriers or obstacles included in the Proposal in the related question on the application. Identify challenges encountered and steps taken to address them throughout the project; and,
- Attend ad hoc webinars, bilateral (online) meetings or other discussions relevant to the project, including field visits by Safe Online team members, as applicable.

Terms & Conditions

- By submitting this proposal, you are authorising End Violence to evaluate the proposal for a potential award, and you agree to the terms herein.
- You agree and acknowledge that personal data submitted as part of the proposal, including name, mailing address, phone number, and email address of you and other named staff in the proposal may be collected, processed, stored and otherwise used by End Violence for the purposes of administering the website, reporting to donors and evaluating the contents of the proposal.
- You acknowledge that neither party is obligated to enter into any official agreement as a result of the proposal submission, End Violence is under no obligation to review or consider the proposal, and neither party acquires any intellectual property rights as a result of submitting the proposal. End Violence reserves the right to withdraw at any time and the applicant agrees to not take any action to bring End Violence into disrepute.
- Applicants represent and warrant that they have authority to submit a proposal in connection with this CFP and grant the rights set forth herein on behalf of their organisation. Any problems that arise related to IP or data privacy are solely the responsibility of the applicant.

- A sample grant confirmation letter with its legal stipulations and conditions is available here for interested applicants.

3. Selection criteria

Eligibility criteria

Only entities that fulfil these mandatory requirements will be considered eligible:

- Your organisation is a **legally registered** entity within the country or countries of implementation. In addition to this, letters of support from local authorities and organisations will also be required, if applicable.
- Your organisation is able to provide **previous auditing records**.
- Your organisation is able to provide a **reference from at least one previous donor or partner**.
- The tech solution addresses **one or more of the four objectives** of the 2021 Open Call.
- The proposed solution responds to a **clear need/gap**, **does not duplicate existing tools**, and/or **builds upon** and/or **interacts with existing solutions**.
- At minimum, an **existing prototype of the solution with promising results from initial pilots**.
- **Funds must not be for** an organisation's core funding, cost of infrastructure, general awareness campaigns, stand-alone research and data collection, activities where a substantial part of the budget is allocated for travel or conferences
- Your organisation has a **safeguarding policy** in place (including data privacy) or is willing to develop a policy. Budget for safeguarding activities up to 5% of the total direct costs.

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 (non-profit or for-profit organisation) in the country or countries of implementation. In addition to this, letters of support from local authorities and organisations will also be required, if applicable.	Yes/No
2. Alignment with priority objectives	The proposed solution addresses one or more of the four objectives set in this Call	Yes/No
3. Builds on existing work	The proposed solution responds to a clear need/gap, does not duplicate existing tools, and builds upon and/or interacts with existing solutions	Yes/No
4. Existing prototype	At minimum, there is an existing prototype of the open-source solution with promising results from initial pilots	Yes/No

5. Safeguarding	The entity has a Safeguarding Policy and procedures in place (including data privacy) or is willing to develop a policy	Yes/No
6. Organisational capacity and references	- Your organisation shall be able to provide auditing records1 - Your organisation shall be able to provide at least one reference from a previous donor or partner	Yes/No

SCORING CRITERIA

Criteria	Specific Criteria	Score
1. Relevance of solution for tackling online CSEA, problem-solution fit	- Alignment between problem described and solution proposed - Relevance of the solution for tackling online CSEA	20 Points
2. Novelty of solution and robustness of prototype	- Generating open source2 technology by: • Developing new technology; • Expanding existing technology; or • Developing a new application / use case of existing technology - Robustness of the results of initial prototyping/ piloting - Existence of code repository	20 Points
3. Suitability of the team and partners to implement the project	- 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	20 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.

2 End Violence will consider occasional exceptions from the open-source rule as justified by the nature and/or sensitivity of the proposed solution. However, all intellectual property and other proprietary rights including, but not limited to, patents, copyrights, and trademarks, with regard to products, processes, inventions, ideas, know-how, or documents and other materials which the Grantee develops using the Grant will be managed in a way that maximises public accessibility and allows the broadest possible use.

	applications with representation from or inclusion of underrepresented populations such as Black, Indigenous and People of Color (BIOPC), Lesbian, gay, bisexual, transgender, queer, intersex + (LGBTQI+), 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 key advisers filling team's expertise gaps - Existence of relevant partners - Existence of consortia with different type of organisations (e.g. local and international, not-for-profit and for profit) or sectors	
4. Likelihood of Impact and Results	- Overall probability of successful delivery of the program and the chance that the predicted impact and results will be realised - Organisation's relevant experience and proof of capacity to implement the project successfully, including solid enumeration of risks and assumptions - A solid methodology for the implementation of the project - Gender mainstreaming incorporated in the design and implementation of the project - A clear Theory of Change and well-articulated monitoring and evaluation plan	20 Points
5. Local buy-in and sustainability approach	- Support Government system strengthening and sustainability - Active involvement of local partners in the design and delivery of activities - Strengthening of local capacity (including under-represented capabilities) through the project to foster local expertise and ensure adequate national capacity and sustainable progress. - When possible, include new models to support and empower local experts in technology, social media, children outreach and other relevant areas to contribute creating a local expertise that understand	10 Points

	their unique context to help combat online CSEA - There is a sound sustainability plan or considerations reflected in the proposal for the continuation of activities and results after the project implementation.	
6. Budget and Value for Money	- The matching of overall budget ask for Safe Online' s investment with main objectives of the project - The balance of funding sources: entity's own capital contribution to the project (human, capital, assets) and other investments - The balance of funding sources: entity's own contribution to the project (human, capital, assets) and other investments -	10 points
TOTAL SCORE		100 Points

More background:

Global Partnership to End Violence Against Children

The End Violence Partnership is a public-private partnership launched by the UN Secretary-General in 2016 to accelerate progress towards Sustainable Development Goal 16.2: ending all forms of violence against children by 2030. End Violence comprises 600+ partners, including governments, civil society organisations, UN agencies, the private sector and research institutions, and acts as a global platform for advocacy, evidence-based action, and investments to end all forms of violence against children.

Through its Safe Online investment initiative, End Violence provides funding, policy and advocacy guidance, and coalition-building to significantly advance national, regional and global efforts to prevent and respond to online CSEA. In 2021, End Violence's Safe Online investment portfolio reached US$48 million in grants to projects achieving tangible results in nearly 70 countries.

Safe Online's grant portfolio as of August 2021 can be found here.

ANNEX I: Online CSEA – the nature, threat and scale of the problem

Online CSEA is a grave and growing problem that requires urgent action.
One out of every three internet users worldwide is a child. Every day nearly 200,000 children go online for the first time. Their lives are shaped by experiences and interactions that are happening online -friendships, entertainment, learning - which are increasingly governed by commercial interest and engagement rules on platforms that have not been designed with children's interest and safety in mind.

Any child can become a victim. Online violence can affect children from all social backgrounds and from any country. Online CSEA is one of the worst manifestations of the failures to ensure children's safety online. It is a growing problem and it needs urgent, collective and global action. Online communities of child abusers are proliferating, many children are coerced or extorted into producing sexualised images or engaging in sexual activities via webcams. Online harm against children, including through the viewing of Child Sexual Abuse Material (CSAM), can be as severe in its impact as abuse committed offline, and in some cases can facilitate the transition to contact abuse. The photos and videos shared on online platforms can harm children for life, and have a direct impact on their development, health and ability to learn and fulfill their full potential.

The statistics are alarming. The numbers of violent and sexual images and videos of children uploaded, or live-streamed on the Internet and Dark Web are increasing at an incredible speed. For instance, the number of reported photos and images received by NCMEC (National Center for Missing and Exploited Children) grew nearly tenfold in 3 years, from 1.1 million in 2014 to 10.2 million by 2017, and doubled again by 2020 with 21.8 million reports received. The Canadian Centre for Child Protection's Project Arachnid web crawler has so far detected 40.7 million images requiring review by their analysts. The monthly number of unique images requiring review currently stands at 100,000 and rising.

CSAM produced by children themselves is a particular concern. Children may share sexual content with their peers or be coerced or otherwise groomed by an adult to produce sexual images and videos. In the first six months of 2020, 44% of all CSAM reported to the Internet Watch Foundation involved material produced by children. As reflected in NetClean's 2018 report, self-produced material is a common feature of law enforcement investigations into online CSEA.

How does online CSEA happen? Three common scenarios:

1. *An adult takes photos or films sexual acts* involving children with a camera or a smartphone and uses them for self-pleasure, sells them for financial gain, shares them on online fora with other adults with sexual interest in children, or uses them to blackmail the child in exchange of money or sexual favours.

2. *The sexual abuse of a child is live-streamed*. Adults with sexual interest in children do not need to travel, they can sit in their house in front of a computer, tablet or mobile phone and abuse the child for their sexual pleasure. It affects mostly children living in poverty and in most cases an adult well-known to the child facilitates the abuse in exchange for money.

3. *A child takes photos or makes videos with sexual content* and shares them via a mobile phone or the Internet with a peer or with an adult. These self-generated images and videos are often used to intimidate or blackmail the child in exchange for money, favours or to pressure them to produce more sexual content or to have sex in real life. This is commonly referred to as grooming, sexting, sextortion, sexual harassment, revenge porn, etc.

ANNEX II: Examples of technology solutions for each objective

Objective 1: **Detect, remove and refer to known and new CSAM, including self-generated CSAM in open and closed online environments and mobile networks**	• expansion and universalisation of hash-based filtering of CSAM • use of crawlers to detect and refer content for removal • Artificial Intelligence (AI) to detect, classify and refer known CSAM • AI to detect conversations and behaviour that may indicate (new) CSAM is shared • tools to detect and distinguish between adult and child language and behaviour to prevent the self-generation and sharing of CSAM and to refer the child to appropriate guidance or services • establishment or strengthening of reporting mechanism (hotlines or other) for CSAM and/or other forms of online and offline CSEA, with national and international referral channels to facilitate removal and appropriate referral of illegal content • forward-looking solutions for detecting all forms of CSEA in emerging environments such as extended reality (XR)
Objective 2: **Prevent and disrupt online sexual grooming of children in digital environments**	• lexicon-based, machine learning algorithms and text analysis of chat room conversations to detect online sexual grooming • online platforms and games to raise awareness of digital dangers • natural language processing (NLP) chatbots to alert the sites' administrator of the suspected grooming, and/or to pre-empt children if online grooming is suspected and offer real-time support via redirecting the child to appropriate services • tools such as age verification that assist in excluding inappropriate membership of child-friendly environments
Objective 3: **Prevent and disrupt the live streaming of child sexual abuse**	• tools for detecting suspected CSEA in live video and peer-to-peer environments • tools to detect, block and/or refer transactions before they occur, for instance via identifying and disrupting patterns of migration from one platform to another e.g. for introductions, online CSEA and payment • tools to disrupt financial transactions and refer victims and/or offenders and potential offenders to appropriate services • establishing or strengthening reporting mechanisms to ensure anonymous reporting of known and suspected live streaming activities

Objective 4: **Expand tools and services to prevent the victimisation of children and harmful behaviour by offenders and potential offenders in digital environment**	• chatbots, online helplines with instant messaging, AI powered services, etc. to provide services for children including CSEA victims, and possibly offenders and adults with a sexual interest in children • establishment or strengthening of helplines and/or (self-) referral mechanisms for offenders and people with a sexual interest in children, including through international exchange of expertise