WEB

Safe & Wise

Creating a better digital world with children

ChildFund Alliance

ChildFund Alliance

Eleven child-focused development agencies are part of the global ChildFund Alliance network, which helps children and their families overcome poverty and the underlying conditions that prevent children from reaching their full potential.

Together we reach nearly 23 million children and family members in 70 countries. Members work to end violence and exploitation against children; provide expertise in emergencies and disasters to ease the harmful impact on children and their communities; and engage children, families and communities to create lasting change.

Our commitment, resources, innovation, knowledge and expertise serve as a powerful force to transform the lives of children around the world.

Members of ChildFund Alliance

ChildFund Australia
ChildFund Deutschland
ChildFund International
ChildFund Japan
ChildFund Korea
ChildFund New Zealand
Barnfonden (Sweden)
Children Believe (Canada)
Educo (Spain)
Un Enfant par la Main (France)
WeWorld (Italy)

May 2022

ChildFund Alliance
545 Fifth Avenue, Suite 1402 New York, NY 10017

+1.212.697.0859
info@childfundalliance.org
childfundalliance.org

WEB Safe & Wise: Creating a better digital world with children, prepared by ChildFund Alliance Secretariat and the ChildFund Online Safety Group.

Cover image: Children using technology as part of ChildFund Laos' education programs

Executive Summary

Over the last three decades, significant progress has been made in advancing children's rights to survival, opportunity, and protection, and in ensuring young people can be heard on matters affecting their lives.

The rapid expansion in digital technologies, however, is now exposing children to an increasing range of threats to their safety and wellbeing.

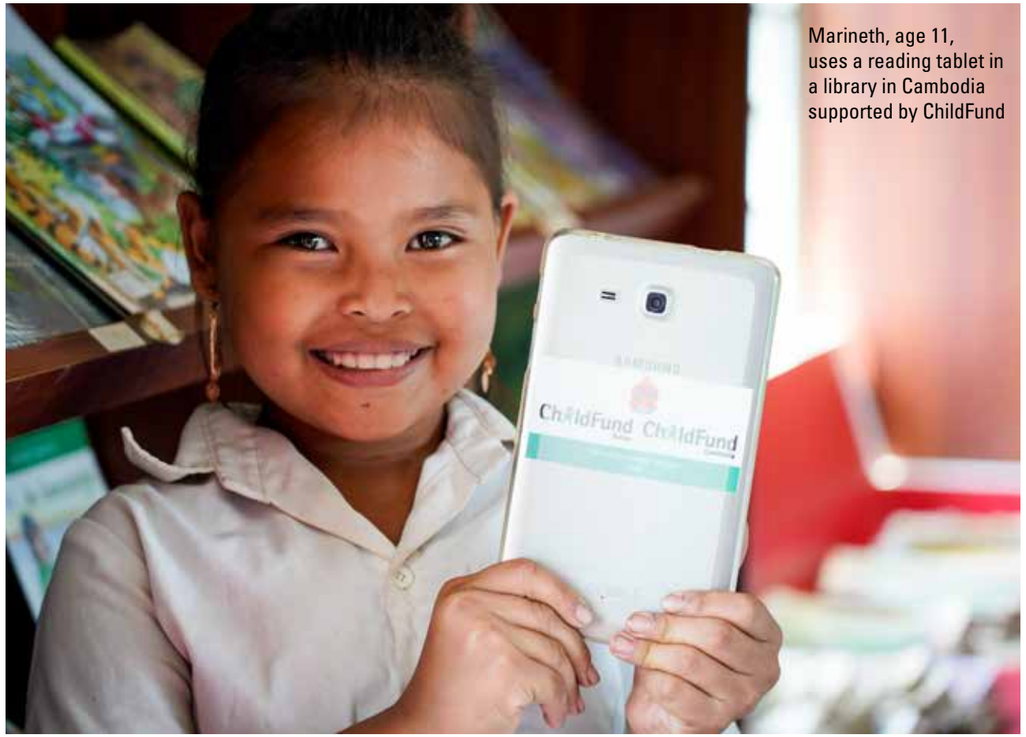
Globally, laws and policies to keep young people safe online are insufficient and inconsistent. This threatens children's ability to access the positive benefits the internet offers, while also being protected from potential dangers.

Further, the extent of harm caused by online connectivity can be exacerbated by a range of contextual factors, such as children's resilience, parental guidance and support, and a child's level of digital literacy.

ChildFund has a long-standing commitment to ending violence against children. Over the next four years, our global strategy will focus on addressing the risks emerging in the digital environment, while empowering children and young people to become effective digital citizens. This will require their access to information and learning, and exposure to skills to use technology safely and responsibly.

Our efforts will include the expansion of digital literacy and online safety programming in the countries where we work, and the launch of our WEB Safe & Wise campaign. **Our global advocacy initiative will focus on driving stronger laws and policies to protect children from online child sexual exploitation and abuse and efforts to help them become effective digital citizens.**

ChildFund believes all children have a right to be safe online. Our overarching goal is to increase awareness, education, and regulation to enhance children's online experiences while keeping them safe from predators.



Marineth, age 11, uses a reading tablet in a library in Cambodia supported by ChildFund

Situation Overview

Paula, age 9, using digital technologies as part of a primary education program supported by ChildFund in Timor-Leste

Since the adoption of the United Nations Convention on the Rights of the Child (UNCRC) in 1989, the world's most widely ratified human rights treaty, the implementation of new laws and policies have resulted in unprecedented improvements in the lives of children and young people.

These advancements in protections have occurred primarily in physical environments and have not fully been extended to the digital environment.

It is estimated that a child goes online for the first time every half second,[1] with more than 200,000 children using the internet daily, and around 800 million actively engaged on social media.[2]

The uploading and live streaming of online child sexual exploitation and abuse (OCSEA) material[3] has increased at an alarming rate.[4]

Coinciding with COVID-19-related lockdowns and school closures, even more children have moved online to learn, play and socialize.[5]

However, alongside the risks of internet connectivity are substantial benefits for young people. Online engagement can provide increased opportunities for children's participation in formal and informal learning experiences, civic engagement, and the creation and sharing of ideas and content with their peers, communities, and decision-makers.

Online platforms can also support children in developing their sense of identity and belonging, and help to build peer, family, intergenerational and community relationships.

Children online: a balancing act

Digital connectivity presents an opportunity to improve children's lives by increasing their access to information and learning resources, and by expanding opportunities for social and civic engagement.

Conversely, it represents a risk to children's health and wellbeing. The expansion of digital technologies and platforms have fostered an environment where perpetrators have the power to abuse, groom, and exploit children.

Advancements to infrastructure, network coverage, and peer-to-peer networks have been driven by commercial interests and do not adequately consider a child's best interests.

These technological advancements, coupled with the expansion of the Dark Web,[6] have changed how offenders produce and share child sexual abuse material (CSAM), leading to increased livestreaming and on-demand OCSEA.[7]

Children living in vulnerable or marginalized situations can be more susceptible to extortion and manipulation, and often have fewer resources at home to protect them from online threats. Many young people have insufficient awareness of the risks they face, and technological advancements constantly outpace regulations intended to protect them.

In the past few years, however, there have been some positive advances in policies and laws (see legislative protections below).

Where effective laws and policies do exist, however, enforcement is often inconsistent, as law enforcement agencies seldom have the human and financial resources, technical capacity, and appropriate legal tools to investigate cybercrimes.

There also remains an urgent need to create a uniform process for referrals between child protection actors and law enforcement, and to ensure resources are available to protect children and support child survivors of online abuse.

Legislative protections for children online

In 2007, the European Council developed the European Convention on the *Protection of Children against Sexual Exploitation and Sexual Abuse,*[8] known as the Lanzarote Convention.

In 2020, the International Telecommunications Union (ITU) updated its *Guidelines on Child Online Protection*.[9]

In 2021, the United Nations published *General comment No. 25 on children's rights in relation to the digital environment*.[10]

In 2021, Germany introduced *The Act to Amend the Network Enforcement Act*[11] to combat online hate speech and fake news in social networks.

In 2021, Australia introduced the *Online Safety Act*[12] which extends the reach of the *Broadcasting Services Amendment (online services) Act 1999* to allow the issuing of removal notices, link deletion notices and app removal notices in relation to child sexual exploitation and abuse material. It also provides for the creation of industry codes of practice.

Digital rights for children

Healthy childhoods are the foundation for the development of healthy behaviors and practices and lead to sustainable and thriving societies.

The *United Nations Convention on the Rights of the Child* (UNCRC) is one of the most rapidly ratified human rights treaties in the history of the United Nations.

It became law in 1990 and serves as the foundation for the provision, protection, and participation of children. This coincided with the public release of the source code for the world's first web browser.[13]

At that time, no one could have predicted the impact the internet would have on society as a whole and specifically on children and young people.

Three decades later, in order to live up to our commitments enshrined in the UNCRC, we must equally respect children's rights online as well as offline. Access to digital devices or connectivity is not yet a guaranteed right for children, which heightens existing inequalities.[14]

Affordable and reliable access to technology, the internet and public services will bridge the digital divide and allow for children to have increased and consistent opportunities to develop their digital skills safely and healthily.

While the UNCRC is the most comprehensive guide to children's rights, it does not implicitly cover the digital environment, which is why *General comment No. 25* is significant.

General comments provide a comprehensive basis to address evolving thematic issues, evidence-based provisions, and suggested approaches for modernizing and implementing treaties.

General comment No. 25 substantiates that children's rights apply equally both online and offline. It also makes concrete recommendations on how to harmonize laws and policies while promoting, respecting, and protecting children's rights in the digital environment.

The benefits and risks for children's engagement online	
BENEFITS	RISKS
Formal and informal learning	Exposure to harmful online content
Information	Misinformation/disinformation
Health literacy	Online child sexual exploitation and abuse
Civic engagement	Cyber-bullying
Identity and belonging	Privacy violations
Peer, family, intergenerational and community relationships	Harassment
Play and recreation	Grooming
Youth employment opportunities	Sextortion

Valuing children's ideas

All children, including those from vulnerable and marginalized situations, have the right to contribute their views and solutions to the design, delivery and evaluation of legislation, policies, products, and services that affect their safety and ensure the fulfillment of their needs and rights in the digital environment.

Children have voices, and their ideas add value. Article 12 of the UNCRC stipulates the right of children to have their views considered in decisions affecting their lives: "States Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child ... in accordance with the age and maturity of the child."

General comment No. 20 (2016) on the implementation of the rights of the child during adolescence[15] advances the guidance on children's participation and calls upon governments to ensure adolescents contribute to the development, implementation and monitoring of all relevant legislation, policies, services, and programs affecting their lives.

Children's digital citizenship,[16] and their ability to use technology, affords them both safety and empowerment in realizing their right to participate online. However, many reasons exist as to why children are unable to reach or access the required skills to engage in safe online environments.

Inequitable global technological access, and the cost of digital devices, can mean their ability to participate online is simply out of reach. Where internet connectivity is available, the digital literacy knowledge gaps of their parents, caregivers and educators can mean they are exposed to dangers while online.

Understanding how the digital world works, even where a child's ability to access it is limited, is still essential to preventing harmful situations from occurring. It also helps ensure young people are equipped with the necessary tools so they can protect themselves once they do venture into digital environments.[17]

Digital libraries are a feature of ChildFund's education programs in Laos

ChildFund: protecting children online

In February 2022, ChildFund Alliance released a four-year strategic plan that reasserts our long-standing commitment to ending violence against children (EVAC).

Our #FreefromViolence campaign, launched in 2016, played a key role in securing the United Nations Sustainable Development Goal Target 16.2: end the abuse, exploitation, trafficking and all forms of violence against and torture of children.

Our goal now is to build upon our past advocacy work by tackling new and evolving risks that are currently affecting millions of children, and which will likely affect exponentially more children in the future if left unaddressed. Above all else, as the world experiences continued disruption and upheaval, we need a strengthened focus on protecting children, their rights, and their wellbeing more than ever before.

Our first priority, identified in our strategic plan, is to examine the rise in risks to children online. This will require a balance between mitigating the mounting dangers they face in an ever more connected world, while simultaneously supporting and empowering children to benefit from opportunities in a digital environment.

Across the globe increased access to the digital world, lack of online safeguards, and low awareness of risks amongst children and their caregivers make children particularly vulnerable to online threats. Further, the extent of harm caused depends on many factors, such as children's resilience, parental guidance and support, and a child's level of digital skills, such as knowing how to manage privacy settings.

To address the increasing threats children face online, ChildFund Alliance will build on our programming and advocacy efforts, leverage existing collaborations, and create new partnerships with those committed to ending violence against children online.

We will raise awareness focused on the areas of prevention, protection, and participation, and mobilize key stakeholders to help children reach their full potential.

Programmatic response

In the latter part of 2021, ChildFund conducted an online safety mapping exercise across its membership to identify the work underway to address online violence. Evidence shows that over 80% of programs took place in the global south, and include the following initiatives:

In Benin, we developed a digital training model for the protection of children, adolescents, and young people from violence on the internet and learning resources to help them safely navigate online.

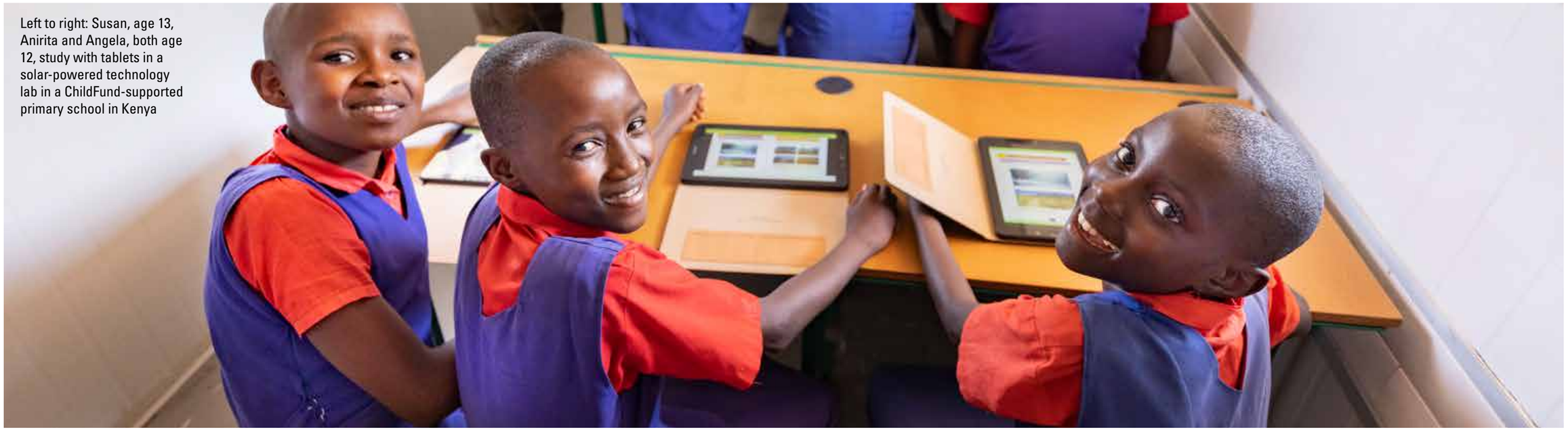
In Ecuador, ChildFund created a digital education program promoted by Fundación Telefónica Movistar to increase digital literacy and support children's development of 21st century skills. This program reached more than 60,000 teachers, 100,000 students, and 700 schools. We also supported the development of a pact between the Government of Ecuador and children and adolescents with the aim of protecting their rights, dignity, and comprehensive development to achieve a secure internet.

In Japan, we are participating in an initiative to expand the national Child Rights Act to include online safety and establish a Child Rights Regulatory Authority with direct responsibility for online safety including removing child sexual abuse material (CSAM) from the digital environment.

In the Republic of Korea, ChildFund is supporting an education program implemented by primary and middle school teachers, community center teachers, and library program facilitators that aims to increase children's and adolescents' digital citizenship.

In Vietnam, we established an innovative program aimed at preventing the online abuse and exploitation of children and teaching youth core competencies to be safe online. The program works with schools to create safe learning environments and mobilizes parents, youth, educators, and the private sector to play an active role in strengthening children's online safety.

A preliminary snapshot of countries with ChildFund online safety programs can be found in Annex 1 (page 12).



Left to right: Susan, age 13, Anirita and Angela, both age 12, study with tablets in a solar-powered technology lab in a ChildFund-supported primary school in Kenya

WEB Safe & Wise: an online safety campaign

ChildFund Alliance is committed to building an accessible, safe, and inclusive digital world for all children and young people based on an ecological framework that requires governments, industry, community members and families to take action.

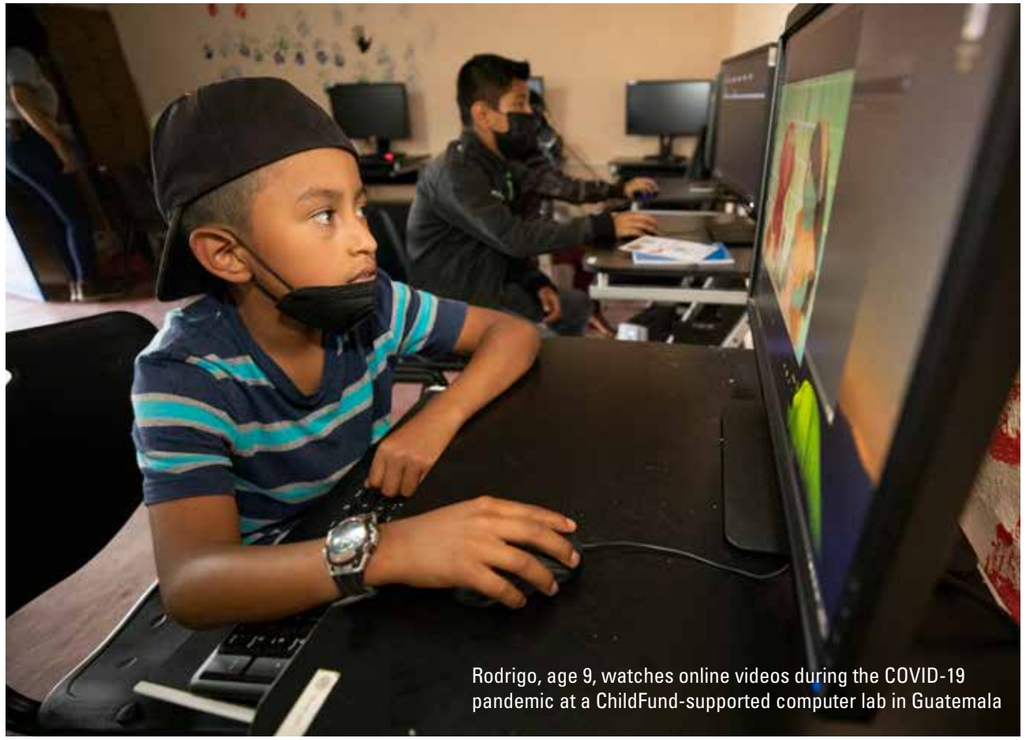
Our WEB Safe & Wise advocacy campaign is focused on two outcomes; laws and policies to protect children from online child sexual exploitation and abuse are strengthened; and children are effective digital citizens who are equipped to participate in online civic engagement safely, ethically, and responsibly as part of their healthy development.

Over the course of this global initiative, we will work with government authorities at the global, national, and sub-national level, leaders in the tech industry and the broader digital community, and with civil society, to advance these calls to action.

We will join with partners to promote these policy asks and mobilize key stakeholders. Based on decades of global programming experience, we are also cognizant that preventing and addressing online child exploitation will have limited impact unless we consider children and their communities as a critical part of the solution.

By launching WEB Safe & Wise, it is our hope and intention that governments, the tech industry, and other stakeholders involved in the protection and participation of children in the digital environment will adopt these asks, transforming the way they approach, coordinate, budget, allocate resources to, and criminalize online abuses against children.

Across low, middle and high-income country contexts, ChildFund seeks global policy asks to improve protections, and support digital skills development and citizenship.



Rodrigo, age 9, watches online videos during the COVID-19 pandemic at a ChildFund-supported computer lab in Guatemala

1. Child Protection

To national government authorities:

1.1 Allocate a mandated ministry and/or lead agency to lead cross-governmental coordination to prevent online harms against children through awareness raising, education, and regulation.

1.2 Develop, strengthen, and enforce comprehensive laws that criminalize online child sexual exploitation and abuse acts (OCSEA) including, but not limited to sextortion, online grooming, and livestreaming of child sexual abuse.

1.3 Strengthen and resource existing child protection systems to incorporate online elements of violence against children and ensure that adequately resourced end-to-end social support services are available for all child survivors of online child sexual exploitation and abuse.

1.4 Allocate resources nationally during budget processes to develop training programs for parents and caregivers, frontline workers, and service providers on how to identify, report and respond to child online safety risks and suspected OCSEA.

To tech industry leaders:

1.5 Develop mandatory industry codes in consultation with young people to safeguard them online and protect them from age-inappropriate content across platforms and providers.

2. Child Participation

To national government authorities:

2.1 Prioritize resourcing for stable, wide-reaching, and affordable internet connectivity and reliable electricity infrastructure so that all children and young people have the access required to develop the necessary protective behaviors to stay safe online.

2.2 Adopt quality online safety curricula in formal and informal education settings and across urban and remote locations that develop core digital competencies (e.g., using privacy settings, understanding the permanency of online content) and good digital citizenship.

2.3 Create more community-based mechanisms for child safe disclosure and reporting of OCSEA, including parenting or youth groups linked to formal child protection systems.

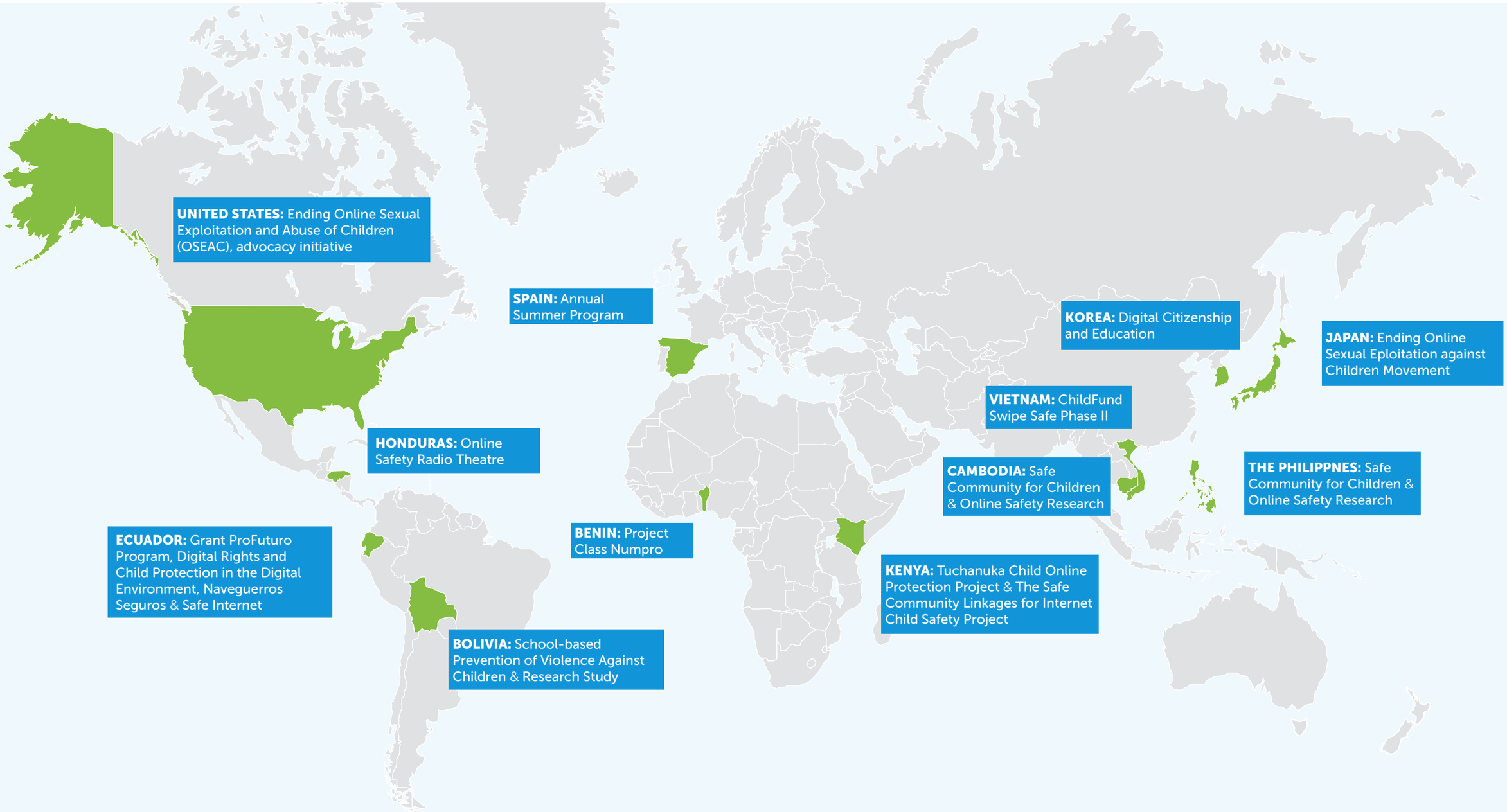
2.4 Invest in dedicated development programs for children and young people that educate them about consent, healthy relationships and how to disclose abuse safely.

To civil society:

2.5 Conduct periodic research of children's online experiences to inform policy, programming, and resourcing decisions. At a minimum, such research should document children's levels of digital literacy and their family's access to and use of digital technology.

Annex 1

Snapshot of ChildFund Online Safety Programs



Key Definitions

Bullying, including Cyber-Bullying: Unwanted aggressive behavior by another child or group of children who are neither siblings nor in a romantic relationship with the victim. It involves repeated physical, psychological, or social harm, and often takes place in schools and other settings where children gather, and online.

Child protection systems: Formal and informal structures, functions, and capacities that have been assembled to prevent and respond to violence, abuse, neglect, and exploitation of children. Most important are the relationships and interactions between and among components and actors within the system.[18] A child protection system is generally agreed to comprise the following components: human resources, finance, laws and policies, governance, monitoring, and data collection, as well as protection and response services and care management. It also includes different actors – children, families, communities, those working at subnational or national level and those working internationally.

Child sexual abuse material (CSAM): Sometimes referred to as 'child pornography,' CSAM refers to material depicting acts of sexual abuse and/or focusing on the genitalia of the child. Child sexual exploitation material (CSEM) encompasses all sexualized material depicting children, including child sexual abuse material. The distinction between CSEM and CSAM is generally one of legal status. A decade ago, there were less than one million reports of CSAM. By 2019, that number had climbed to 70 million, a nearly 50 percent increase over figures reported in 2018. Many more remain undetected.

Digital citizen: A person using information technology in order to engage in society, politics, and government. Effective digital citizenship is being responsible, safe, and effective on the internet and digital devices.

Digital divide: The gulf between those who have ready access to computers and the internet, and those who do not.

Digital literacy: The ability to use information and communication technologies to find, evaluate, create, and communicate information, requiring both cognitive and technical skills.

Livestreaming of online child sexual abuse: Involves the coercion of a child to participate in sexual activities, alone or with other persons. The sexual activity is, at the same time, transmitted live or 'streamed' over the internet and watched by others remotely, often those who have requested and/or paid for the sexual abuse of the child, sometimes dictating how the act should be carried out. This crime transcends national borders allowing perpetrators to abuse their victims from any location.

Online Child Sexual Exploitation and Abuse (OCSEA): Sexual exploitation or abuse of children which is partly or entirely facilitated by technology, for example over the internet or other wireless communications. It can include sexual exploitation that is carried out while the victim is online; identifying and/or grooming potential child victims online with a view to exploiting them sexually; or the distribution, dissemination, importing, exporting, offering, selling, or possession of, or knowingly attaining access to, child sexual exploitation material online.

Online grooming: This is a tactic used by perpetrators to establish and build a trusting relationship with a child using the internet or other digital technologies in order to manipulate, exploit and abuse them online and/or offline.

Online sexual harassment: Unwelcome sexual advances, requests or demands for a sexual favor, and other verbal or physical conduct of a sexual nature. 'Sexual harassment' refers not only to sexual conduct with the explicit intention to violate the dignity of another person, but also conduct of a sexual nature that a person experiences as offensive or intimidating.

Sextortion: Where an individual is blackmailed using self-generated, explicit images of that person in order to extort sexual acts, money, or other benefits from her/him. The blackmailer typically threatens to share the material without the consent of the depicted person, for example by posting the images on social media. Children or young people may be coerced into continuing to produce sexual material and/or told to perform distressing acts under threat of exposure to others of the material. In some instances, the abuse spirals so out of control that victims have attempted to self-harm or commit suicide as the only way of escaping it.

Footnotes

[1] UNICEF: www.unicef.org/protection/violence-against-children-online

[2] The Global Partnership and Fund to End Violence Against Children: www.end-violence.org/safe-online

[3] Disrupting Harm, research by ECPAT International, INTERPOL and UNICEF: www.interpol.int/en/Crimes/Crimes-against-children/Projects-to-protect-children/Disrupting-Harm

[4] Global Threat Assessment 2019, WeProtect Global Alliance: www.end-violence.org/sites/default/files/paragraphs/download/Global%20Threat%20Assessment%202019.pdf

[5] Coronavirus Disease (COVID-19) and Its Implications for Protecting Children Online, UNICEF: www.unicef.org/documents/covid-19-and-implications-protecting-children-online

[6] Dark web definition, Merriam Webster: www.merriam-webster.com/dictionary/dark%20web

[7] Child exploitation, EUROPOL: www.europol.europa.eu/crime-areas-and-statistics/crime-areas/child-sexual-exploitation

[8] Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention), Council of Europe: https://rm.coe.int/protection-of-children-against-sexual-exploitation-and-sexual-abuse/1680794e97

[9] The Guidelines on Child Online Protection, co-authored by the International Telecommunication Union: https://www.itu-cop-guidelines.com

[10] General comment No. 25 (2021) on children's rights in relation to the digital environment, Office of the High Commissioner for Human Rights: www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

[11] Act to Amend the Network Enforcement Act, Bundeministerium der Justiz: www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/Bgbl_NetzDG.pdf;jsessionid=D4DE27B32DEEC4B8B1910FE6781E8324.1_cid334?__blob=publicationFile&v=2

[12] Online Safety Act 2021, Australian Government: www.legislation.gov.au/Details/C2021A00076

[13] History of the Web, World Wide Web Foundation: https://webfoundation.org/about/vision/history-of-the-web

[14] Children and young people's rights in the digital age: an emerging agenda, University of Western Sydney: https://researchdirect.westernsydney.edu.au/islandora/object/uws:38531

[15] General comment No. 20 (2016) on the implementation of the rights of the child during adolescence, United Nations: https://digitallibrary.un.org/record/855544?ln=en

[16] 21st Century Children as Digital Citizens, OECD: www.oecd.org/education/ceri/21st-Century-Children-as-Digital-Citizens.pdf

[17] Children and young people's rights in the digital age: an emerging agenda, University of Western Sydney: https://researchdirect.westernsydney.edu.au/islandora/object/uws:38531

[18] A Better Way to Protect all Children, UNICEF, UNHCR, Save the Children, World Vision: https://fecongd.org/pdf/crianca/BetterWayProtectChildrenUNICEF2012.pdf

ChildFund supports out-of-school youth in Kiribati through its Building Blocks program

ChildFund®

Every child deserves to live a life free from violence.

childfundalliance.org