WEB Safe & Wise

Creating a better digital world with children

NATIONAL ADVOCACY TOOLKIT

ChildFund® Alliance

WEB Safe & Wise National Advocacy Toolkit

ChildFund Alliance is a global network of 11 child-focused development and humanitarian organizations reaching more than 32 million children and their family members in 70 countries.

Our 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)

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

+1.212.697.0859
rdesouza@childfundalliance.org
www.childfundalliance.org

Prepared by Dr. Lorleen Farrugia, A1 Research, and Ryan De Souza, ChildFund Alliance

Contents

WEB Safe & Wise: *Creating a better digital world with children*

During the last three decades, we have seen significant progress in advancing children's rights to survival, opportunity, and protection, as well as their right to speak on matters affecting their lives.

A key factor in improving the well-being of children and youth is digital connectivity, which has increased access to information, learning resources, and expanded opportunities for social and civic engagement. Conversely, the rapid expansion in online technologies is exposing children to an increasing range of threats to their safety.

These threats include, but are not limited to, exposure to harmful content online, misinformation/disinformation, online child sexual exploitation and abuse, cyberbullying, privacy violations, grooming, and sextortion.

Globally, laws and policies to keep young people safe online are insufficient and inconsistent. While some countries have made important strides in protecting children online through legislation and policies, online child sexual abuse and exploitation and harmful content is not always adequately defined, and identification of perpetrators too often relies on community policing. Further, many laws pre-date technological advances, and are not adaptive to the global and ever-evolving nature of the internet.

These weaknesses in regulation threaten children's ability to access the positive benefits the digital world offers, while also being protected from potential dangers.

As part of ChildFund Alliance's FY22-25 Strategic Plan, Working Together to Address Emerging Threats to Children's Safety, we have launched WEB Safe & Wise. This new initiative focuses on addressing the risks emerging in new technologies, while empowering children and young people to become effective digital citizens. ChildFund launched the initiative in May 2022 during an event with subject matter experts.

ChildFund recognizes that all children have a right to be safe online. We are committed to building an accessible, safe, and inclusive digital world for all children and young people based on a framework that requires governments, industry, community members, and families to take action.

Our WEB Safe & Wise advocacy campaign is focused on two key outcomes:

- Laws and policies to protect children from online child sexual exploitation and abuse are strengthened.
- Children are effective digital citizens who are equipped to participate in online civic engagement safely, ethically, and responsibly as part of their healthy development.

To achieve these outcomes, ChildFund has identified a number of global policy asks that are designed to improve protections and support digital skills development and citizenship.

1. Child Protection	2. Child Participation
To national government authorities:	***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.	**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.
1.2 Develop, strengthen, and enforce comprehensive laws that criminalize online child sexual exploitation and abuse (OCSEA) acts including, but not limited to, sextortion, online grooming, and livestreaming of child sexual abuse.	**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.
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.	**2.3** Create more community-based mechanisms for child safe disclosure and reporting of online child sexual exploitation and abuse, including parenting or youth groups linked to formal child protection systems.
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 online child sexual exploitation and abuse.	**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 tech industry leaders:	***To civil society:***
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.	**2.5** 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.

ChildFund® Alliance

free from violence and exploitation

Foreword

ChildFund Alliance has a long-standing commitment to ending violence against children. We know that we cannot end child poverty unless we also address the abuse and exploitation of children in their homes, at school, and within society.

Prioritizing the creation of safe environments for children was the cornerstone of our *Free From Violence* campaign, where ChildFund Alliance and its members advocated for the inclusion of a specific target in the post-2015 development agenda. These efforts contributed to the establishment of Goal 16.2 within the Sustainable Development Goals: ending the abuse, exploitation, trafficking, and all forms of violence against and torture of children.

Today, our members continue to implement programs to address a wide range of child protection issues. This includes building safe and inclusive learning environments, eliminating harmful traditional practices such as early marriage, and providing safe spaces during humanitarian conflict.

Working in partnership with young people, parents, community leaders, governments, and civil society, we are seeing good signs of progress. In recent years, however, new threats to children's safety are emerging as young people increasingly engage with the online world. It is vital that young people have the opportunity to engage with digital technologies, which offer valuable spaces in which to learn, connect, and develop new skills and knowledge. But we must also ensure that they are protected from harm.

More than 175,000 additional children go online for the first time every day, and we are witnessing an alarming increase in online child sexual exploitation and abuse as a result. ChildFund Alliance's Web Safe and Wise Advocacy Campaign has been developed in response to these new threats, and has two primary aims:

- to advocate for new, or strengthened, laws and policies to protect children while online; and
- to equip children with the skills and knowledge needed for them to become effective digital citizens, empowered to participate online safely, ethically, and responsibly.

This toolkit has been developed to support ChildFund Alliance members and their country offices in advocating for safer online environments for children. We hope this is a useful resource and welcome your feedback on ways it can be improved.

The most successful advocacy campaign begins with small steps. Your efforts to drive change at a local or national level will help children in your region, but also support our global efforts. Together, by building a groundswell of action, we can create a better digital world for children.

Meg Gardinier

Meg Gardinier, Secretary General
ChildFund Alliance

Overview of the toolkit

Unlike cigarettes, alcohol and junk food, the use of new media and technology does not come with warning signs about the potential risks and harms associated with tech use. While an individual can carry on their day-to-day life easily without any of the former three, it is very difficult to do so without using technology.

In today's world, technology is pervasive in everyday life. Yet online safety is often an afterthought, particularly where children are concerned. To further complicate matters, online safety is a very young field, and advocates often feel at a loss about how to approach it. The increasing use of devices, applications and tools by children and young people for leisure, connectivity, and education, makes online safety a crucial aspect that must be addressed.

This Toolkit aims to provide a practical and accessible approach to online safety advocacy, allowing online safety advocates among ChildFund Alliance members to:

1. gain a deeper understanding of online safety advocacy;
2. access common tools for creating, rolling out and updating their advocacy strategies; and
3. strengthen their capacity for online safety activities.

We acknowledge and understand that national online safety advocacy efforts will differ in the regions where ChildFund Alliance members operate. As such, this toolkit has been designed using a a modular approach, so that it can be used by country offices taking their first steps into campaigning, as well as those which have already developed an advocacy strategy.

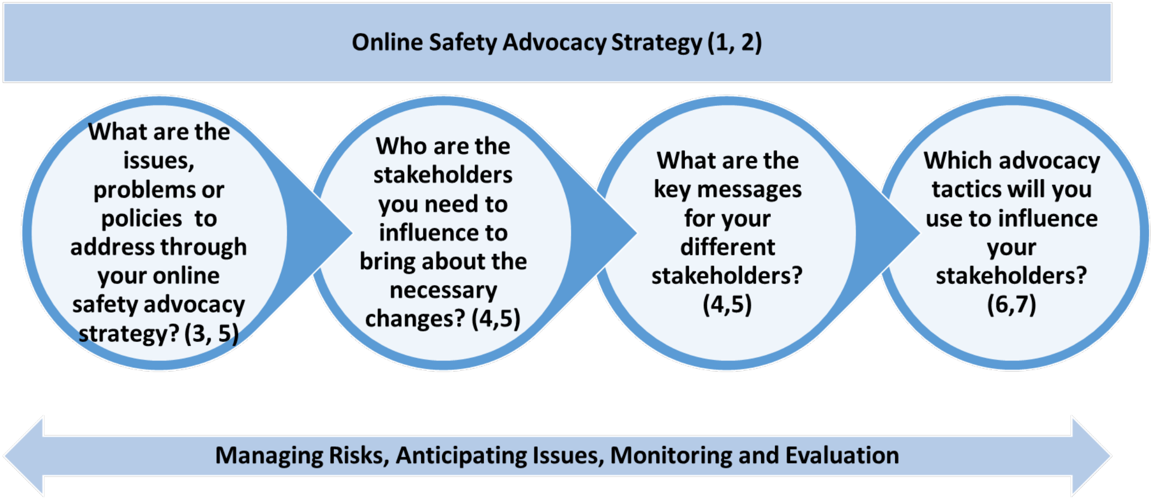

Online Safety Advocacy Strategy (1, 2)
What are the issues, problems or policies to address through your online safety advocacy strategy? (3, 5)
Who are the stakeholders you need to influence to bring about the necessary changes? (4,5)
What are the key messages for your different stakeholders? (4,5)
Which advocacy tactics will you use to influence your stakeholders? (6,7)
Managing Risks, Anticipating Issues, Monitoring and Evaluation

Figure 1: Online Safety Advocacy Toolkit: using the modules

Module 1: will help you deepen your understanding of online safety and the risks that children and young people face online, using the CO:RE classification: content, contact, conduct, contract, and crosscutting risks. This module also includes a glossary of key online safety terms, and detailed information on children's online activities and the issues they face.

Module 2: will help you develop an advocacy strategy and implementation plan. This module provides information on how change can be achieved, why children are specifically in need of advocacy, and the eight key principles for campaigning. We also explain the four phases of advocacy - assessment, planning, implementation, and evaluation – and provide tools to help you implement each phase.

Module 3: will help you identify key issues to include within your advocacy strategy. This includes deepening your understanding of the local context, sourcing research and data, and assessing the quality of this evidence. We also show you how quality research can be used to develop an evidence-based advocacy strategy.

Module 4: will help you identify key stakeholders, understand their power and influence, and learn how to engage them within your advocacy strategy. This module also provides guidance on how to construct convincing messages, which target the different key stakeholders, identified.

Module 5: the WEB Safe and Wise campaign has 10 high-level policy asks which focus on the two key areas of child protection and child participation. This module will provide guidance on policy analysis, so that you can find existing policies, identify any policy gaps, and determine where existing polices need strengthening or reinforcement.

Module 6: offers a range of advocacy tactics, including tools specific to campaigning, using traditional and social media, lobbying and negotiating, establishing partnerships, and engaging communities. We share examples of good practices from ChildFund Alliance members and provide tools to help you choose the right tactics for each targeted change and the role of your stakeholders.

Module 7: explains how online safety issues intersect with other child protection issues, such as poverty, climate change, conflict and terrorism, natural disasters, pandemics and economic crises. This will help you integrate online safety advocacy within other advocacy efforts to ensure the best use of their existing resources.

Module 8: In the final section of the toolkit, we share a case study based on the advocacy experiences of ChildFund Ecuador. It highlights how they acknowledge their important role as child advocates in the country, and their efforts to influence different levels of the State, society, and families to contribute to a framework for the protection of children and adolescents against violence in the digital world, particularly sexual violence, through the safe use of the Internet.

Throughout the online safety advocacy process, it is important to keep in mind the risks that can arise, and anticipate possible issues, such as child safeguarding requirements when the participation of young people is being sought as part of the advocacy strategy. The toolkit should also link to each organisation's Monitoring and Evaluation Framework, with the Theory of Change and Results Framework identifying milestones and targets for the advocacy strategy.

Human and financial resources to implement an advocacy campaign might not always be accessible. The resources included here are as cost-effective as possible, and the toolkit includes a section on how online safety advocacy can be incorporated within other project and activities targeting child protection. We hope that you find this toolkit useful in your online safety advocacy. Please remember to get in touch with the ChildFund Alliance Secretariat if you need our support.

Module 1: Understanding online safety

1.1 Definition of online safety

Online safety refers to an awareness and understanding of the threats that exist in the digital environment and having the requisite skills and knowledge to identify them, and engage in preventative measures in order to stay safe online and avoid such threats.

The online environment keeps changing rapidly, but there are some basic concepts of how to keep safe online:

- protecting our personal information,
- guarding against viruses, malware and other security threats,
- avoiding content that makes us feel uncomfortable, or that is illegal or harmful, and
- behaving appropriately when engaging in online communication.

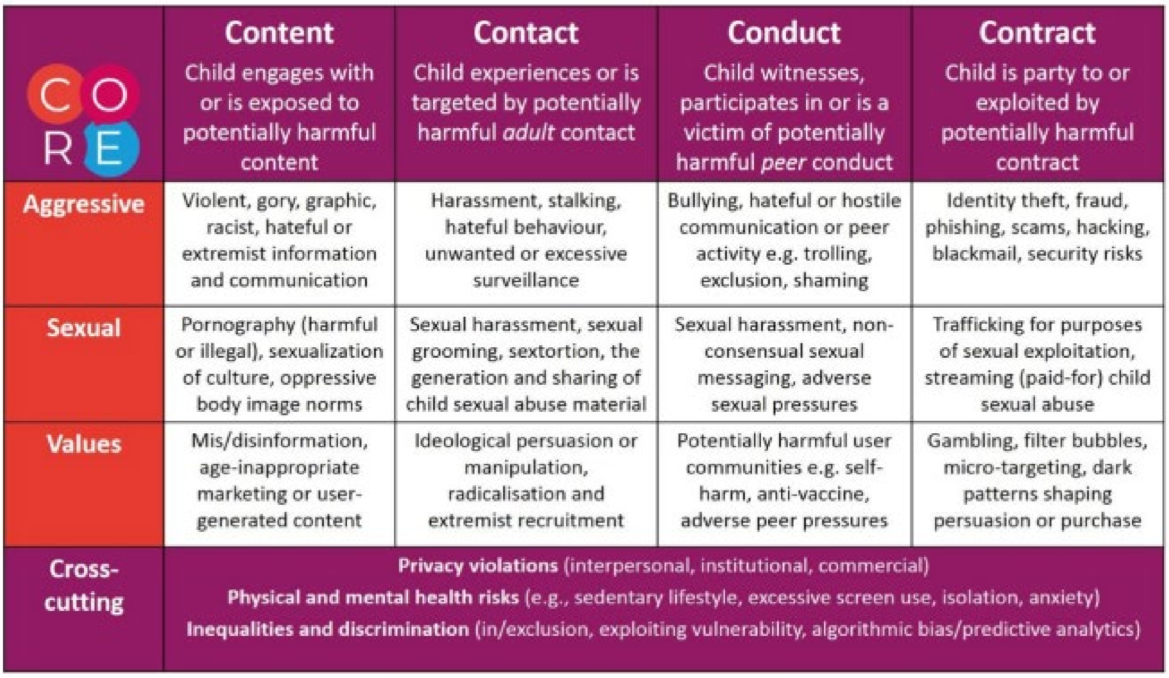
Awareness, education, information, and technology are all important components of online safety[1], which can also be referred to as 'internet safety', 'e-safety' and 'cyber safety'. Cybersecurity, on the other hand, involves the protection of one's devices and networks from third party attacks. [2]

The EU Kids Online network[3] presented a child-centred approach to classify online risks into three main categories: content risks, contact risks, and conduct risks. Online risks were classified according to two dimensions:

- The role of the child. For example, whether they were on the receiving end of online content; a participant in online activities instigated by adults; or an actor in peer-to-peer exchanges online.
- The nature and extent of online risk they face.
- These classifications provided a much-needed understanding of online risks and became a reference point for policy-makers and practitioners worldwide.

Further, developments in the digital environment have highlighted the commercial risks children can be exposed to. This has led to a fourth category of online risks: contract risks. This includes, for example, when children sign up for digital services, and accept terms and conditions, without sufficient awareness that this relationship can be unfair or exploitative.[4]

The classification of online threats also includes three crosscutting risks: privacy, mental and physical health, and inequality and discrimination. Figure 2 below portrays this classification of online risks as presented by Livingstone & Stoilova (2021)[4].



CO RE	**Content** Child engages with or is exposed to potentially harmful content	**Contact** Child experiences or is targeted by potentially harmful *adult* contact	**Conduct** Child witnesses, participates in or is a victim of potentially harmful *peer* conduct	**Contract** Child is party to or exploited by potentially harmful contract
Aggressive	Violent, gory, graphic, racist, hateful or extremist information and communication	Harassment, stalking, hateful behaviour, unwanted or excessive surveillance	Bullying, hateful or hostile communication or peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, hacking, blackmail, security risks
Sexual	Pornography (harmful or illegal), sexualization of culture, oppressive body image norms	Sexual harassment, sexual grooming, sextortion, the generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messaging, adverse sexual pressures	Trafficking for purposes of sexual exploitation, streaming (paid-for) child sexual abuse
Values	Mis/disinformation, age-inappropriate marketing or user-generated content	Ideological persuasion or manipulation, radicalisation and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, adverse peer pressures	Gambling, filter bubbles, micro-targeting, dark patterns shaping persuasion or purchase
Cross-cutting	**Privacy violations** (interpersonal, institutional, commercial) **Physical and mental health risks** (e.g., sedentary lifestyle, excessive screen use, isolation, anxiety) **Inequalities and discrimination** (in/exclusion, exploiting vulnerability, algorithmic bias/predictive analytics)			

Figure 2: The CO:RE Classification of Online Risk to Children

To address online safety in a comprehensive way, understanding the multiple risks that exist for children is vital. Moreover, these risks exist and function within the several contexts that surround children, including families, peers, educators, legislation, industry and the cultural context, among several others.

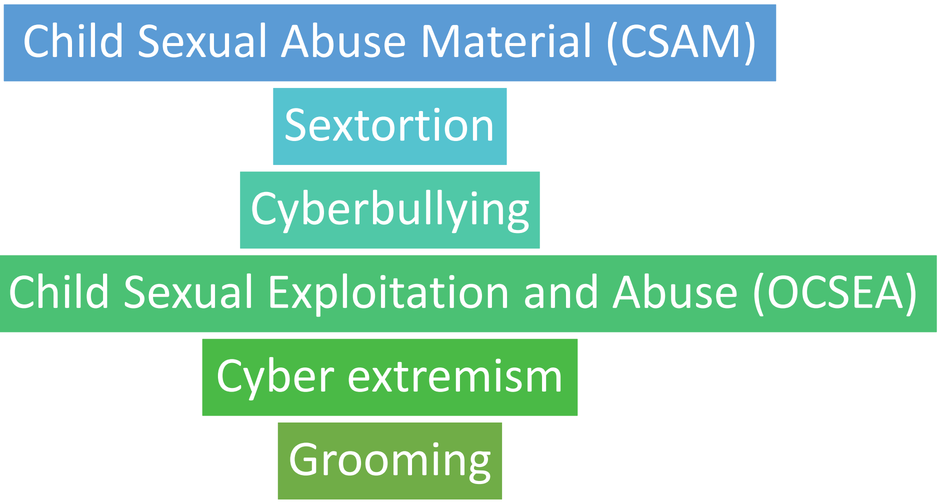
These contexts can also influence the way children interact within the online environment, the online risks they may be vulnerable to, and how they approach online safety. Children cannot be held solely responsible for their safety online. As part of the factors that can influence how children relate to online risks, these contexts also need to be part of the solution and assume the shared responsibility for keeping children safe online.[5]

This is a key message for advocacy efforts. All stakeholders share a part of this responsibility. For children to be protected, all stakeholders must be engaged to act within their field of responsibility.

1.2 Key terms and definitions

There are various terms related to online safety, and it is useful to be familiar with them and their definitions when promoting online safety advocacy. This will help you understand and convey to stakeholders the relevance of the issues and the implications of the dangers children can face online. Familiarise yourself with these terms. Figure 3 presents some of the key terms and acronyms. A full glossary with definitions is presented in Appendix A.

Keep in mind that in some cases, these terms might not translate directly into local language, and you will need to identify the best way to translate these concepts.



Child Sexual Abuse Material (CSAM)

Sextortion

Cyberbullying

Online Child Sexual Exploitation and Abuse (OCSEA)

Cyber extremism

Grooming

Figure 3: Key terms related to online risks

Module 2: Advocacy

This module presents you with information about advocacy, the principles that guide advocacy, and an outline of the advocacy process which will help you develop your strategy.

2.1 What is advocacy?

All people, including children, have a voice. Advocacy provides a platform for these voices and aims to ensure that people are heard on issues in order to bring about change. Advocacy also aims to ensure that:

- people understand their rights,
- human rights are protected and promoted,
- the views and rights of those concerned are taken into consideration in any decision-making processes related to them;
- individuals are empowered to voice their views and concerns about matters that affect them,
- data and evidence is available to support to issues being tackled, and
- necessary societal changes are identified and promoted.

In relation to these objectives, advocacy involves taking actions on multiple levels to influence decision-makers and those who hold executive and legislative powers to bring about the necessary changes related to the issue.

Advocacy efforts also have the potential to have a wider impact. An organisation that tries to create change can choose to work directly with their target groups. This is impactful up to a certain extent. When an organisation also works in the field of advocacy, the changes can potentially be much greater and have a larger impact with a wider target group.

For instance, a group of parents can work to ensure their children's school is well equipped to deal with situations of bullying. However, if this group of parents also engages in advocacy in relation to the issue of bullying with relevant stakeholders, such as the institutions that train teachers, the impact of their advocacy efforts can reach beyond their own school.

Advocacy can bring about different types of changes. The Anne Casey Foundation[6] outlines the following types of changes that can be achieved:

Table 1: Types of change

Type of Change	What Changes?	Example
Shift in Social Norms	Changes in knowledge, attitudes, values and behaviors within society.	The public's awareness of the importance online safety issues increases.
Strengthened Organizational Capacity	Improved organizational conditions such as training, staffing, funding of those organizations that can bring about change.	Non-governmental organizations in the field of online safety are trained in strategic planning.
Strengthened Alliances	Changes in the relationships and alliances within those structures that have common goals.	Establishing partnerships with national and international organizations working on the eradication of OCSEA.
Strengthened Base of Support	Changes in the level and type of support within the public, opinion leaders and other interest groups.	Gaining the support of child protection organizations towards online safety issues.
Improved Policies	Establishment of new policies, the development of existing ones and the adoption or implementation of such policies.	A national scientific research study about online safety issues is carried out in the country to update an existing policy based on the relevant evidence. Development of new legislation is also another possible outcome.
Changes in Impact	Changes in the lives and conditions of those individuals or groups targeted by the advocacy efforts.	The online safety policy is implemented through direct interventions within the community, engaging community support, and behavioral changes happen as a result.

Coffman and Beer (2015)[7] identify three points on the change continuum, which reflect different types of engagement stakeholders have with the issues being presented to them. These are:

- Awareness: becoming aware that an issue or a problem exists. Although this is important, it is usually insufficient to bring about change.
- Will: increasing the will to act on an issue or problem. This is an interim stage between awareness and action, where the awareness develops into an understanding of the urgency and relevance of the issue that is a further step towards action.
- Action: taking action on the specific issue or problem.

Why do children need advocacy?

While we teach children to be their own self-advocates, they are still developing and have evolving capacities. In addition, in the digital space, they are rarely able to advocate for themselves as they may not have the opportunity to directly influence decisions being made about them. This online space poses new risks to children who can become targets of online abuse.

The United Nations Convention on the Rights of the Child (UNCRC)[8] is the most widely ratified treaty worldwide and defines the specific rights of children. These are based on the seminal principles of non-discrimination, the best interests of the child, the right to life, survival and development, and the right to participate and be heard.[9]

The UN General Comment No. 25 (2021)[10] translates how these rights apply in the digital environment. Online safety advocacy is necessary to ensure that children's rights online are protected and upheld, so that children can enjoy and benefit from online opportunities while staying safe.

2.2 Principles of advocacy

The APSP[11] outlines six principles that should guide advocacy. These are credibility, transparency and accountability, participation, communication legitimacy, and human-rights focused.

Given the participative nature of online safety advocacy, inclusion, equality and non-discrimination, together with being ethical and applying safeguarding principles, are also important. These principles ensure that the relevant structures and practices are in place to maximise your potential for advocacy.

Table 2 presents these principles together with a brief checklist for you to review how your organisation is applying these principles.

Table 2: Principles of Advocacy

Principle	Definition	Checklist
Credibility	This refers to your organisation's trustworthiness	How do you ensure honesty and truthfulness in your work? Are you using established and reliable sources to base your advocacy efforts on?
Transparency and Accountability	Transparency involves sharing information with the relevant target groups. Accountability means assuming responsibility for the actions you are taking and their outcomes.	Are you sharing information about your advocacy efforts with those you are advocating for? Is the way your organization is governed, your management strategies, and decision-making processes sufficiently clear?
Participation: "nothing about us without us"	Participation involves engaging the beneficiaries of your advocacy efforts in the process. It ensures that your advocacy is child-centered and that children's voices are truly listened to and responsibly conveyed to the relevant stakeholders in your advocacy messages.	Are you engaging children in your advocacy strategy? How are you ensuring that through child participation children's voices about online safety are being put forward through your advocacy strategy? In what way can you ensure that children's needs are being adequately and accurately conveyed to your stakeholders?
Communication	Advocacy is about communicating key messages to different stakeholders through the appropriate channels.	What tools and resources do you have available to construct your advocacy messages?
Legitimacy	Legitimacy is gained by being involved in the issues you are advocating for, and by working with those who are impacted by these issues or those who identify with the same cause.	In what way is your organization involved in online safety advocacy? Who are the experts in your organization that can contribute most to online safety? How can you convince your stakeholders of your legitimacy in this field? Why should they listen to you?
Human-rights focused	Advocacy that is based on human rights treaties (such as the UNCRC) increases the influence of your work, and exerts the relevant pressures on duty bearers to fulfil their obligations in view of such charters.	Is your organization following a specific human or child rights treaty or convention? How can you link these rights to your advocacy process? How are children and their rights included in the advocacy process?
Inclusive, ensuring equality and non-discrimination	This ensures that children from all contexts and backgrounds are listened to and included in the advocacy strategy.	Are you aware of the situation of all children in your country? How are you ensuring that your advocacy practices are inclusive and non-discriminatory?
Ethical and adhering to safeguarding principles	Advocacy should adhere to the ethical standards of beneficence, respect for all persons and justice to ensure that children do not encounter any forms of abuse or harm through their involvement in the advocacy process.	What ethical frameworks is your organization abiding by? What specific child safeguarding plans do you have in place or need to consider when children are participants in your advocacy? How can you ensure that children are not harmed through their involvement in the advocacy process?

2.3 The advocacy process

Advocacy can be considered a cyclical process (Figure 4) that begins with an analysis and understanding of the current situation to identify which issues or problems need to be addressed. The process of planning the advocacy strategy, which is then implemented in the subsequent phase, follows this.

Throughout this cycle, it is essential to establish a project monitoring framework that gives you the flexibility to correct your course if there is any part of your process that is not achieving its intended outcomes.

Finally, the advocacy process should be evaluated according to the established Theory of Change and Results Framework to assess the outcomes identified.

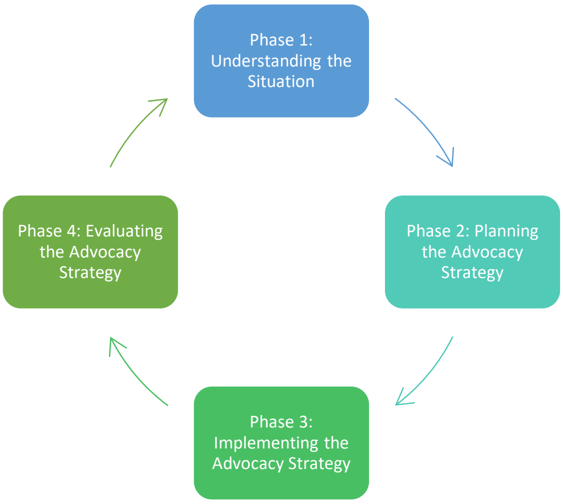

Phase 1: Understanding the Situation
Phase 2: Planning the Advocacy Strategy
Phase 3: Implementing the Advocacy Strategy
Phase 4: Evaluating the Advocacy Strategy

Figure 4: The advocacy process

Phase 1: Understanding the situation
This first phase can involve multiple aspects, including an assessment of the local context related to the issue (see Module 3 and Module 5), identifying different types of change e.g. policy and legislative change, and identifying the relevant stakeholders that have the power to bring about change in relation to these issues (Module 4). When advocates have a clear understanding of the situation, it helps you set specific objectives, which are very useful in designing the subsequent phases of the advocacy process.

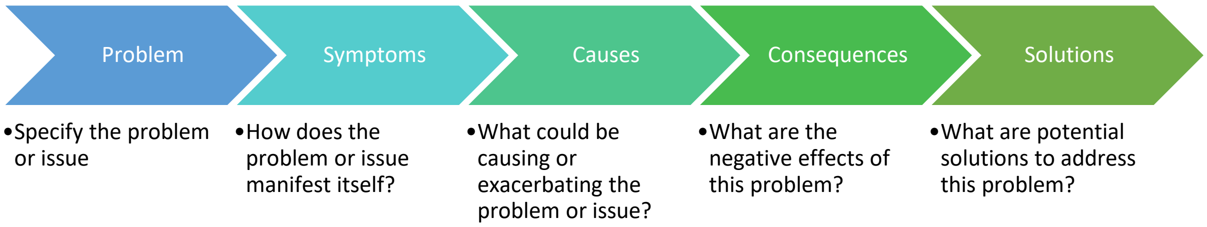
Phase 2: Planning the advocacy strategy
The second phase of the advocacy process involves planning the advocacy strategy. Here it is important to ask several questions to set the goals for your advocacy strategy.

Some of these questions can include:

- What is the change that you want to achieve?
- How can this change be achieved?
- What are the key messages?
- Who are the stakeholders who have the power to help create this change? (Module 4)
- How can you deliver messages and evidence to them in the most effective way? (Module 6)
- What resources are available to you?
- What are the key milestones you need to reach to achieve these goals?

A clear grasp of the situation (Phase 1) will help you identify several issues or problems that need to be addressed. Engaging in a problem analysis can help you assess the nature of the problems or issues to identify possible solutions. This is crucial to the advocacy-planning phase.

One way of conducting a problem analysis is portrayed below (Figure 5). For each problem or issue identified in the first phase, follow these steps. It helps you assess the nature of the issue, how it manifests itself, what could be causing it, whom it is affecting negatively and how, and potential solutions to address this problem. This problem assessment helps you answer key questions in the advocacy planning stage and contributes to defining your advocacy strategy.


Problem
- Specify the problem or issue

Symptoms
- How does the problem or issue manifest itself?

Causes
- What could be causing or exacerbating the problem or issue?

Consequences
- What are the negative effects of this problem?

Solutions
- What are potential solutions to address this problem?

Figure 5: Problem analysis

Look at the solutions identified in the planning phase, and reflect on the following questions to help you refine your strategy:

- Is this solution realistic?
- Is this solution feasible?
- Who needs to be engaged in order to implement this solution?
- How can your message be tailored to the specific target audience?
- What are the resources (human, financial, technological, etc…) needed to implement this solution?
- Are these resources accessible to you now?
- What could be the right time to implement this solution?
- Are there other possible solutions to this problem or issue?
- How can the impact of this solution be measured?
- Could this solution have a negative impact?

Remember, you might not be able to tackle all the problems or issues at once. Identify what is most important and establish a priority list. Tackle the most important issues first.

For each problem you are addressing, set SMART goals[12] for your advocacy strategy. This means that your goals should be:

- Specific: targeting a specific area for improvement and identifying how this will be tackled and by whom.
- Measurable: identifying what will be measured to indicate progress.
- Attainable: identifying accessible tools which can help you reach these goals.
- Realistic: ensuring that they can actually be achieved based on the available resources.
- Timely: specifying a timeline within which these goals can be met.

Goals can also be short-term or long-term. Short-term goals can be achieved in a short period, while longer-term goals will take longer to achieve and can be split up into a series of shorter-term goals.

You can use many resources for project management, and you may wish to look at resources already used by your organisation. Gantt Charts can help you prepare a timeline for your advocacy strategy. These show a breakdown of the different components of the project, the timeframe for each component, how one component relates to the other, and the individuals responsible for each component. Figure 6 shows a sample Gantt Chart.

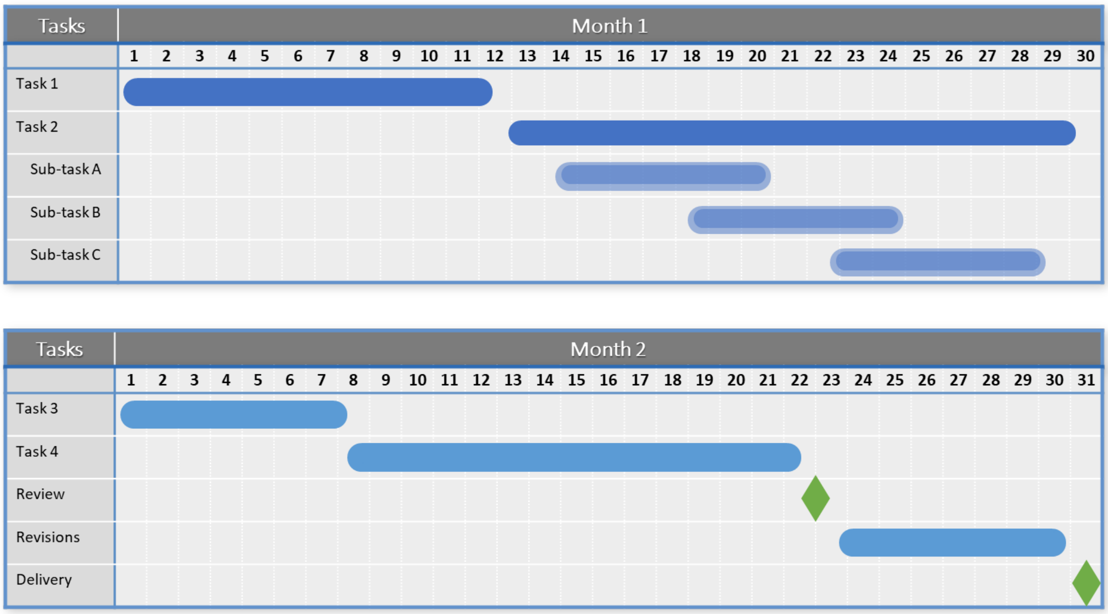


Figure 6: Sample Gantt chart
(source: https://templates.office.com/en-us/two-month-gantt-chart-tm56247502)

Phase 3: Implementing the advocacy strategy
Once the planning phase (Phase 2) is complete, the implementation phase is where the advocacy strategy comes to life. Module 4 will help you identify the relevant stakeholders, learn how to engage with them, and phrase your key messages according to your target stakeholders. Module 6 presents various advocacy tactics you can use, and Module 5 focuses specifically on the use of advocacy to develop policies and laws related to online safety.

Phase 4: Evaluation

The final phase of the advocacy strategy involves the evaluation. Here, you can examine what was successful and what didn't work as expected, how this success is being measured, and how to ensure future advocacy efforts will be successful.

This evaluation will feed into your next advocacy cycle. The context, issues to be addressed, stakeholders, and your advocacy goals are dynamic. Your advocacy efforts need to develop in line with these changes to remain relevant and timely.

Keep in mind that although evaluation is presented as a final stage, it is good practice to structure an ongoing evaluation within the process. Include monitoring and evaluation as part of the planning process. This ensures you remain on track with your plan and if something isn't working, changes can be made.

It is also important to anticipate anything that might go wrong in the advocacy process. One way to go about this is to engage in an advocacy pre-mortem.[7] This is a hypothetical evaluation that occurs at the beginning of your advocacy process where you imagine that your advocacy strategy has already been implemented and was unsuccessful. To carry out this exercise:

1. Ask everyone involved to identify possible reasons for failure.
2. Make a list of all these possible reasons for failure
3. Identify the ones that are most likely to happen.
4. Identify which indicators you need to look out for to identify if there is anything wrong with the strategy.
5. Ensure that your advocacy strategy addresses and anticipates these potential issues.

As part of the advocacy pre-mortem, it is also useful to ask everyone involved to think about:

6. any unforeseen positive thing(s) happening,
7. how they can contribute to achieving the desired changes, and
8. how they could ensure these unforeseen positive elements become part of the advocacy strategy.

Module 3: Mapping the local context

An important step in the advocacy process is the gathering of data and evidence. These help you identify the issues or problems to be addressed and provide the necessary backing to your advocacy claims and strategies. It is important that your advocacy campaign is evidence-based.

Carrying out research is always helpful as it helps assess and monitor the current context. Research takes time and requires resourcing. If you are not in a position to conduct or commission new research, it may be possible to identify research by other organisations that can be applicable for your advocacy strategy. Moreover, if research about online safety issues already exists, it would be counterintuitive to duplicate the work. You could invest more resources towards the advocacy strategy.

This module will help you assess the quality of existing research and establish whether it can be used towards your advocacy strategy. It will also help you identify the main findings of existing research and issues that need to be addressed in your advocacy efforts.
If you are unsure of whether such research exists in your country, Module 4 will also help you engage or establish partnerships with stakeholders, such as higher education institutions or research centres, that might be conducting research on online safety or that can assist you with gathering evidence.

Before you proceed, list what you already know about online safety in your context and identify the source of this information. Use Table 3 to record the research you have available. This helps you identify preliminary knowledge about the online safety context, where your information is derived from, and it can help you assess whether this is a relevant source of information.

Table 3: Current contextual knowledge of online safety

Make a list of any information you know or have about children and online safety in your context.	List the source/s of this knowledge or information.

3.1 Identifying existing evidence

Looking at existing evidence is the best way to start mapping out your context in relation to online safety and to assess the advocacy needs of children in your country. This evidence can be in the form of research studies, reports, surveys, consultations, statistics, and policies, among others.

Locating existing research, information and data about online safety: In your country and within your organization, you likely have developed a network of local and international contacts involved in the thematic. You should hold consultation sessions to identify any gaps in research, information and data.

Search for research online: through existing databases and news portals. You can use some of the keywords presented in the glossary of this toolkit together with the name of your country to identify any research that has been published. You can also set up internet search alerts using these keywords so you are notified when any new research is published.

Examine higher academica publications and research centers: Try to establish partnerships with these institutions or connect to key individuals within them. They will be useful to locate new research and for lobbying. If you have funding available, you may also conduct or commission research in partnership with these entities.

Systematic reviews: are research studies that summarise evidence from multiple studies. These can be very useful as they collate and summarise information in a way that allow you to access the most important findings in one paper. Generally, these reviews are published in academic journals but can also be published as reports. The report by the WHO about what works to prevent online violence against children is one example.

Global comparative research studies: These are usually conducted at a global level by international non-governmental organizations or coalitions and, generally, an institution or individual could be responsible for the governance of the research in your country.

Some examples of such research are the Disrupting Harm research project focusing on OCSEA and the Global Kids Online project that aims to understand the online experiences of children worldwide. Be on the lookout for newly published material and reach out to learn more about these projects and get access to the findings. These studies may help you identify trends in your own country, and you may be able to make comparisons to identify upcoming trends.

Child internet safety helplines and hotlines: These are specific services where children can seek advice about online safety, or where people can report online CSAM. Generally, these helplines collect and publish data about the main issues that children seek help for, indicating the most salient issues children are facing. This can also be useful evidence to analyse for advocacy purposes. Identify your local helpline and hotline and be on the lookout for new reports they publish about their work.

Use Table 4 to create a list of the sources of research, data or evidence that you have identified in your context.

Table 4: Sources of research

Data Sources	Links to Data
Existing research studies, information or data	
Online research databases	
News portals	
Higher education institutions	
Universities	
Research centres	
Systematic reviews	
Comparative research studies	
Internet safety helplines and hotlines	
Other	

3.2 Assessing the quality of research studies

Another important step before deciding which studies to use for your advocacy strategy is to assess the quality of the evidence you have available. These are some key things to look out for:

Relevance: The digital world evolves rapidly, and you need to ensure that the study is addressing relevant issues. The timeliness of the data is also very important.

Reliability, validity and trustworthiness: These aspects are crucial elements in assuring the quality of research studies. Reliability refers to consistency over time and internal consistency, while validity refers to the strength of the study. Trustworthiness is the equivalent of these two concepts in qualitative research.

Authoring: The research quality is often indicated by its author or publisher. Studies published in peer-reviewed journals that have a high impact factor are some of the best quality available. Published reports can also be high quality evidence sources, but it is best to review each publication you identify on its own merit. It is also important to note funding sources as these can help you identify potential issues and conflicts of interest.

Sample: The sample chosen for the study is important to establish the quality of a study. If the study is quantitative, it needs to be a large sample (with the sample size n being greater than 30) that is selected randomly to enable generalisation to the population. A sample for a qualitative study needs to be purposeful to ensure that it really reflects the issues being investigated.

Limitations and Biases: Every research has limitations, and these should be acknowledged and, where possible, addressed through the research. For the same reasons, it is important to identify and address any biases. These can be related to the researchers' biases and blind spots, but also biases that arise from the data collection or the research participants.
Based on each of these aspects, Table 5 presents a checklist that you can use to assess the quality of research studies identified.

Table 5: Assessing the quality of research

NAME OF STUDY:		
Area	**Checklist**	**Answer**
Relevance	Is this study designed specifically to investigate issues related to online safety?	□ YES □ NO
	When was the study conducted? Is it recent enough?	□ YES □ NO
	Does the study reflect the scenario in your country?	□ YES □ NO
Reliability, Validity and Trustworthiness	Is the methodology chosen adequate for the research question being investigated?	□ YES □ NO
	Is the methodology replicable?	□ YES □ NO
	Does the study note the value of Cronbach's Alpha for reliability if a test is being used?	□ YES □ NO
	Can you trust the study's findings?	□ YES □ NO
	If the study is qualitative, does it provide sufficient descriptions of the findings and their context, which is backed up by quotations from the research participants?	□ YES □ NO
Authoring	Can you identify who conducted the study?	□ YES □ NO
	Can you identify who funded the study?	□ YES □ NO
	Can you identify who published the study?	□ YES □ NO
	Can you identify any conflicts of interest?	□ YES □ NO
Sample	Is the sample size large enough?	□ YES □ NO
	Was a random sampling strategy utilized?	□ YES □ NO
	Is the sample representative of all children in the country (including context, and situations) in order to be generalizable?	□ YES □ NO
	Is the sample inclusive of the diversity of children and their online experiences?	□ YES □ NO
Limitations and Biases	Are the limitations acknowledged?	□ YES □ NO
	Are the limitations adequately addressed?	□ YES □ NO
	Are the biases acknowledged?	□ YES □ NO
	Are the biases addressed in some way?	□ YES □ NO
	Are there any evident biases and limitations that are not addressed?	□ YES □ NO

3.3 Using research to identify the issues to address

Once you have established the quality of a research study or source of evidence, the next step would be to focus on how this evidence can be utilised within your advocacy strategy. You can use the Table 6 below to organise information about the different sources you identified. This table summarises the important information and helps you pick out the issues that need to be addressed.

Table 6: Summary of research studies

Source	Which relevant issues does it address?	What are the main findings?	What are the recommendations raised by the research?	Are there any existing research gaps?
1.				
2.				
3.				
4.				
5.				

Once you have summarised this information, look at the main findings and the recommendations for the specific issues and explore how these could be in included in the advocacy strategy. As presented in Module 2, a clear understanding of the current situation is crucial to establish the issues that need to be addressed and help you construct clear key messages for different stakeholders.

The research gaps identified can also be useful for the advocacy strategy. One kind of advocacy is to lobby for further research. Knowing where the research gaps are can help you with this process.

Module 4: Engaging with stakeholders

Stakeholders are people, organisations, or institutions that are involved with, can influence, or care about the issue of online safety. After identifying and prioritising the issues to be addressed, the next step is to carry out stakeholder analysis to identify who the key people and organisations are, what type of power and influence they have, and which issues they can help you address. It is also important to identify how to tailor specific messages to target specific stakeholders. This increases the effectiveness of your advocacy efforts.

ChildFund Alliance members who participated in a survey while preparing this toolkit already interact with a number of stakeholders as part of their online safety programmes. Figure 7 portrays who these stakeholders are and how frequently members of ChildFund Alliance interact with them in their advocacy efforts.

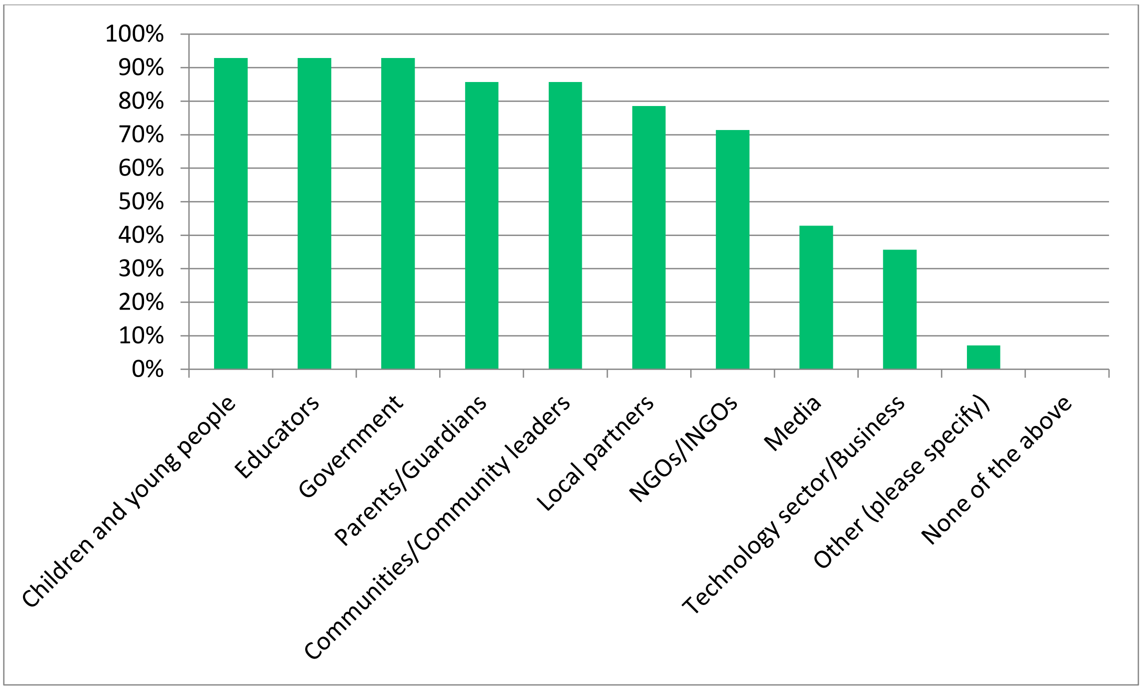


Figure 7: Stakeholders ChildFund Alliance members interact with while working on online safety programs

4.1 Stakeholder and power analysis

Identify individuals and organizations that have an interest in online safety issues and determine who has the power and potential to influence or bring about a change in these issues within your context.

Start by making a list of all those people or groups who can influence or are influenced by online safety issues. You can consult experts or young people themselves in identifying stakeholders. Figure 8 below presents some possible stakeholders in relation to online safety.

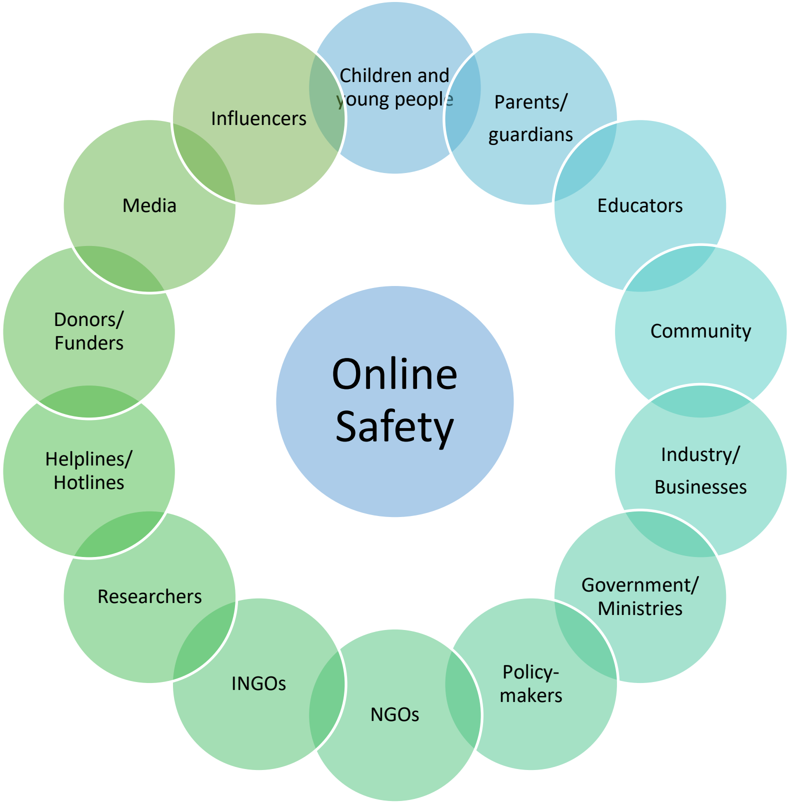


Figure 8: Potential stakeholders

The next step is to identify who these stakeholders are within your national context. Fill in the grid presented in Table 7 to help you list the relevant stakeholders within your country. You might also identify other categories of stakeholders that you want to add to your list.

In the third column, note down any engagement you already have with these stakeholders. This makes it easier to identify where you already have individuals who can be involved in your advocacy efforts, and where you need to establish contacts.

Finally, list whether these stakeholders are members of the public, influencers, or decision-makers. These are the main actors in the policy process. They include the public (e.g., parents or teachers), those who can influence policy (e.g., the media, community leaders,), and finally the decision-makers (e.g., policy-makers within government, members of parliament).[7]

Table 7: Country specific stakeholders

Stakeholder Category	Stakeholders in my context	Contacts	Type of Stakeholder
	List the individuals or organisations in your country/context who are working on online safety for children for each category.	*Include the names of any contacts you already have.*	*Tick ⍰ whether they members of the public, influencers or decision-makers.*
Children and young people			□ Public □ Influencers □ Decision-makers
Parents/guardians			□ Public □ Influencers □ Decision-makers
Educators			□ Public □ Influencers □ Decision-makers
Community			□ Public □ Influencers □ Decision-makers
Industry/ Businesses			□ Public □ Influencers □ Decision-makers
Government			□ Public □ Influencers □ Decision-makers
Policy-makers			□ Public □ Influencers □ Decision-makers
Non-Governmental Organisations (NGOs)			□ Public □ Influencers □ Decision-makers
International Non-Governmental Organizations (INGOs)			□ Public □ Influencers □ Decision-makers
Researchers			□ Public □ Influencers □ Decision-makers

Helplines/Hotlines			□ Public □ Influencers □ Decision-makers
Funders			□ Public □ Influencers □ Decision-makers
Media			□ Public □ Influencers □ Decision-makers
Influencers			□ Public □ Influencers □ Decision-makers
Other Stakeholder/s			□ Public □ Influencers □ Decision-makers

The context in which you are carrying out your advocacy strategy is also important to consider. You can further reflect on your local context by using the acronym PESTLE. Each letter stands for one of the following contexts:

1. Political (e.g., political climate, policies)
2. Economic (e.g., poverty, unemployment)
3. Social (e.g., education, attitudes)
4. Technological (e.g., technological access, skills)
5. Legal (e.g., legislation, enforcement)
6. Environmental (e.g., disasters, conflicts)
7. You can also add the international context to add an international dimension, given the global nature of online safety issues

A PESTLE analysis is a useful strategic planning tool, which helps to identify external risks and opportunities that may directly affect your advocacy strategy.

Understanding these contexts gives you further insights into your advocacy strategy. Here are some examples:

- If there is some awareness in society about the dangers of OCSEA, you might decide to capitalize on this and link your advocacy strategy to anything that is already happening in the public arena.
- An existing government white paper might provide an opportunity for you to comment and respond as part of your advocacy strategy.
- The differences in rural and urban areas when it comes to children's technological access or the availability of support from parents and guardians might need different advocacy approaches.
- If your organisation is already working on other issues, e.g., education, poverty, climate change, you might be able to include online safety advocacy within these strategies (refer to Module 7 for further information about this).

Once you have established a list of stakeholders who are interested in online safety and your country's context, it is now important to identify how much power each holds to influence or make a difference in online safety issues. To help you reflect on this, you can ask some of the following questions:

- What is the role of this stakeholder?
- Why do you think this stakeholder is important?
- What is the stakeholder's interest in online safety?
- What has the stakeholder been doing in the field of online safety?
- What are your experiences, if any, of collaborating with this stakeholder?
- What kind of power or possibility to influence online safety issues does the stakeholder hold?
- How can the stakeholder contribute to your online safety advocacy strategy?
- There are various types of power. The following are some types of power[13, 14] to think about when reflecting on what kind of power your stakeholders have over online safety issues:

Table 8: Types of power

Type of Power	Explanation
Visible power	These are formal power structures and decision-making bodies that one can clearly see. They include rules, institutions, and procedures (e.g., government, legislation).
Invisible power	This includes the ideologies, values, norms, beliefs, and culture that shape our perceptions of the world.
Hidden power	This includes people and institutions in power who have stakes to maintain their influence and position of privilege. They manipulate agendas and exclude the voices of those who are less powerful.
Power to	This refers to individuals' ability to take action related to themselves. Online safety advocacy can also target this kind of power to help individuals nurture skills and qualities to maintain their own safety online.
Power with	This refers to individuals' ability to find common ground, build on their collective strengths and act together. Online safety advocacy can bring together individuals and organisations who share the same interests and develop allegiances that share a common purpose.
Power from within	This is related to an individual's sense of self-worth, self-knowledge and confidence. This can also be referred to as agency, or one's ability to take action towards social change.
Power over	This is the authority or control one has over others and it is not always the most democratic source of power.

These kinds of power can function in different spaces. These may be closed spaces (or those that are relatively inaccessible), invited spaces where individuals are invited to participate, and claimed or self-created spaces. The latter refers to spaces created by communities or movements to address specific concerns.

Power is also found at various levels. Some of your stakeholders will have the power to influence the local context (e.g., an NGO), while others will have the power to influence the national (e.g., the national government) or international context (e.g. the United Nations (UN) or the African Union (AU)).

Power can function in constructive ways that support positive change, but it can also be less constructive and sometime be in direct opposition of any changes you are seeking.

After reflecting on the different stakeholders you have identified and what type of power they might have, it is also useful to conduct a power analysis exercise. This helps you map these stakeholders with how much power they have to influence online safety issues. Through this exercise, you can identify where to focus your advocacy efforts. Figure 9 can help you map the stakeholders you identified according to two dimensions. Dimension 1 (horizontal) relates to whether these stakeholders support your cause or not, while dimension 2 (vertical) is related to the level of power or influence they have over online safety issues you wish to focus on. These would be the issues you have decided to focus on after going through Module 3.

Once you have mapped this out, focus on the quadrant at the top right. These are the stakeholders who support change and those who have more power or influence over the issues. For example, this could be a minister in your government who is already involved in projects related to online safety issues. Clearly, they have the power to influence because of their role, and their previous engagements with online safety issues indicate that they support positive change in relation to these issues.

It is also good to take note of which of your stakeholders might be in the other quadrants. Although your advocacy efforts might not be concentrated with these stakeholders, it is good to be aware of them and identify if they could influence your online safety advocacy in any way, both positively and negatively. You might also want to target some of the stakeholders in the other quadrants to seek specific outcomes. Stakeholders who support your cause but do not have much power or influence can still be helpful to promote your cause. You can also engage in lobbying with an influential organisation which does not yet have a position on online safety issues to get them to change their position and support the cause. It would also be useful to include some risk management strategies in your campaign to prepare for anything that might be unexpected.

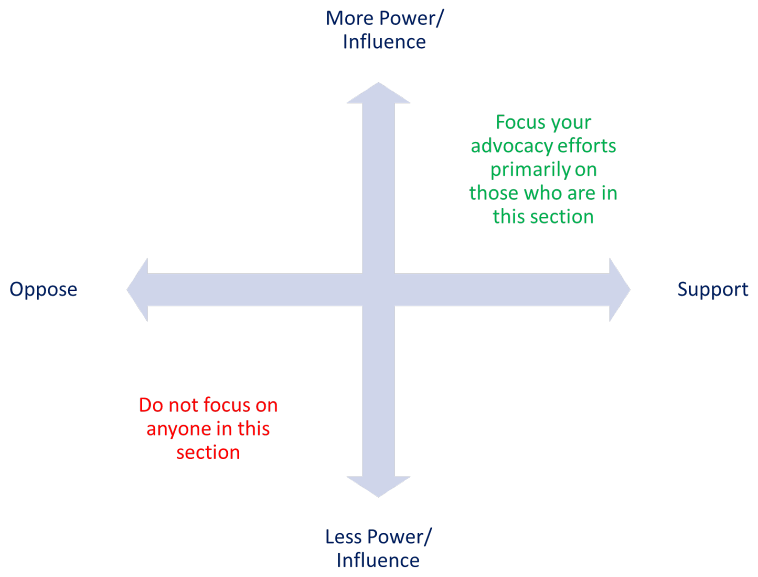

More Power/ Influence
Focus your advocacy efforts primarily on those who are in this section
Oppose
Support
Do not focus on anyone in this section
Less Power/ Influence

Figure 9: Mapping stakeholder power (Adapted from https://rabble.ca/political-action/powermapping/)

Another way to carry out this power analysis is to use Table 9 where you list each stakeholder and mark their agreement with the online safety cause, how important the issue is to them and their level of influence.

Table 9: Stakeholder power analysis (Adapted from www.careemergencytoolkit.org/wp-content/uploads/2017/03/28_10.pdf)

Stakeholder	Agreement							Importance			Influence		
	-3	-2	-1	0	+1	+2	+3	Low	Medium	High	Low	Medium	High
	-3	-2	-1	0	+1	+2	+3	Low	Medium	High	Low	Medium	High
	-3	-2	-1	0	+1	+2	+3	Low	Medium	High	Low	Medium	High
	-3	-2	-1	0	+1	+2	+3	Low	Medium	High	Low	Medium	High
	-3	-2	-1	0	+1	+2	+3	Low	Medium	High	Low	Medium	High
	-3	-2	-1	0	+1	+2	+3	Low	Medium	High	Low	Medium	High

You can also classify whether the stakeholders are members of the public (e.g., young people, teachers), influencers (e.g., media, thought leaders, advisors) or actual decision-makers[7]. This will help you determine which advocacy tactics to adopt when targeting specific stakeholders.

4.2 Constructing a convincing message

Once you have identified the main issues for your advocacy strategy and identified the key stakeholders, it is time to construct your key messages so you can present strong arguments to influence your stakeholders.

Advocacy efforts are generally based on a core message. This is defined as “the most important argument, idea or fact that you need to get across to your different target audiences to win support for your advocacy objectives” (p. 26).[15] The message needs to be clear, focused and expressed in a phrase that can be communicated in various formats.

These different formats will depend on your audience or the different stakeholders. The message can be a full brief where you have the possibility to elaborate and give sufficient details to stakeholders who are invested in the issue. At other times, you might need to be prepared to give your message in the format of an elevator pitch[a]. This is useful for those instances where you have a limited time with a stakeholder and you need to pass on your advocacy message to gauge their interest in a brief but persuasive way.

[a] A brief way of introducing oneself, making a connection, and delivering a key point about your organization or project

To construct a detailed brief[16], make sure to include:

- an explanation of the issue,
- why it needs to be addressed,
- how it can be addressed,
- research findings, data, or other form of evidence that would support your claims,
- what is being done to address the issue,
- what else can be done to address the issue,
- case study or good practice examples, and
- the specific actions that need to be taken

An elevator pitch generally involves:

- an introduction to your work;
- an explanation of what you want; and
- a call to action.

Irrespective of which format you use, keep in mind that good, persuasive advocacy messages are:

- simple clear
- interesting
- noticeable
- focused on solutions
- target specific aspects
- practical
- evidence-based
- adapted for each audience
- generate an emotional response
- appeal to logic reasoning

In the next section, you will identify which messages are suitable for each of your stakeholders.

4.3 Key messages for different stakeholders

Tailoring your messages for different types of stakeholders will ensure your advocacy strategy is more effective. Use the tips in 4.2 and fill in Table 10 to help you devise persuasive messages for your key stakeholders based on the evidence you have gathered.

Table 10: Key messages for the stakeholders

Issue	Stakeholder	Evidence	Key Message/s
Specify the issue or problem you want to address *E.g.,*	*List the different stakeholders* *E.g.,*	*List any evidence or any relevant information that you will use to construct your key message*	*Construct a core persuasive message for each stakeholder*
Increasing awareness of online safety	*1. Decision-makers*		
	2. Media		
	3. General Public		

Various tactics can be used in advocacy campaigns. In addition to constructing the right messages for your target audience, it is also important to choose the correct medium to convey that message. Advocacy tactics are presented in Module 6.

Module 5: Law and policies

Country contexts have to be considered thoroughly where laws and policies are concerned. As advocates for online safety, it is important to be aware of what policies already exist, what is missing, and where one can find tools and resources to build upon existing policies, and strengthen those where there are gaps. Such as the International Telecommunications Union's Child Online Protection Guidelines for Policy-Makers, a user-friendly and flexible framework that supports the development of targeted and effective measures for child online protection at the national level.

Groups, organisations or governments consider policies as plans, ideas, as guidelines for decision-making or as commitments to pursue a specific course of action that has been officially agreed upon. Policies can function at local, national or international levels, and some policies develop into laws.

As part of the WEB Safe and Wise campaign, ChildFund Alliance has 10 high-level policy asks which will form the nucleus of the work throughout the campaign. The policy asks presented below focus on two key areas: child protection and child participation.

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.

These high-policy asks are directly related to the key messages you want to develop for the relevant stakeholders.

5.1 Policy analysis

Knowing what policies already exist in your country, and carrying out an assessment of these policies, is important to help you devise your advocacy strategy. This step goes hand-in-hand with Module 3. Existing policies are also important in mapping out your country's context.

With reference to the 10 high-level policy asks developed by ChildFund Alliance, fill in Table 11 to establish, A) whether these policies are present or underway in your country, B) if they are being implemented properly, and C) whether there are any known issues that need to be addressed. Tick Yes, No or I Don't Know for questions A, B and C for each of the ten high-policy asks and in column D add any relevant comments about your answers.

Table 11: Assessment of existing policies

High-policy Ask	**A. Is this present / in progress in your country?**			**B. Is this adequately implemented in your country?**			**C. Are there any known issues in relation to this high-policy ask?**			**D. Comments**
	Yes	No	Don't Know	Yes	No	Don't Know	Yes	No	Don't Know	
1. Child Protection										
1.1										
1.2										
1.3										
1.4										
1.5										
2. Child Participation										
2.1										
2.2										
2.3										
2.4										
2.5										

After completing this table, you will be able to see where there are gaps in relation to the policy asks in your country. If there are questions you do not know the answer to, seek to obtain the relevant information first in order to be able to answer Yes or No. The comments that you have written in column D will help you identify any issues in relation to each policy ask, and these can be addressed through your advocacy strategy.

Once you have filled in this table, the flowchart in Figure 9 helps you track the progress on each of these policy asks and suggests possible advocacy strategies you can adopt. These strategies are presented in more details in the subsequent sections of this module.

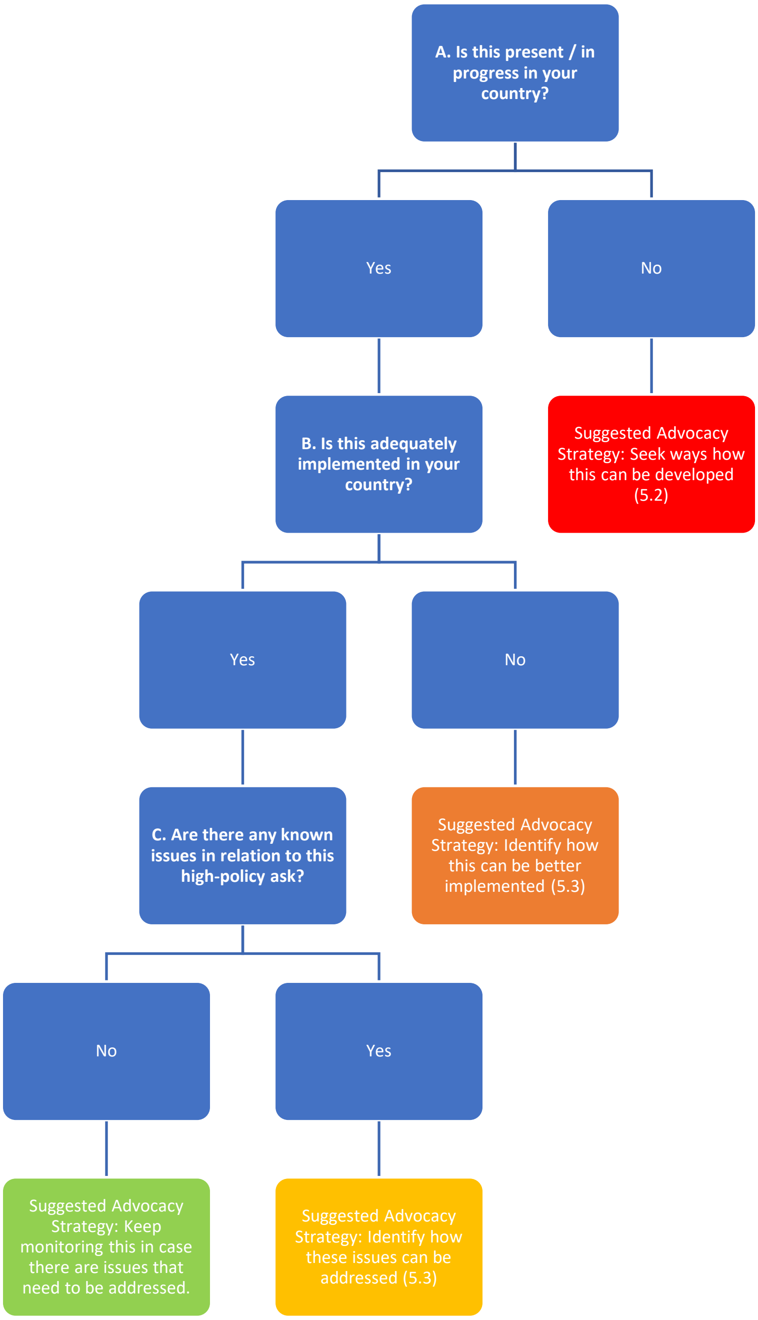

A. Is this present / in progress in your country?
Yes
No
B. Is this adequately implemented in your country?
Suggested Advocacy Strategy: Seek ways how this can be developed (5.2)
Yes
No
C. Are there any known issues in relation to this high-policy ask?
Suggested Advocacy Strategy: Identify how this can be better implemented (5.3)
No
Yes
Suggested Advocacy Strategy: Keep monitoring this in case there are issues that need to be addressed.
Suggested Advocacy Strategy: Identify how these issues can be addressed (5.3)

Figure 10: Policy status flowchart

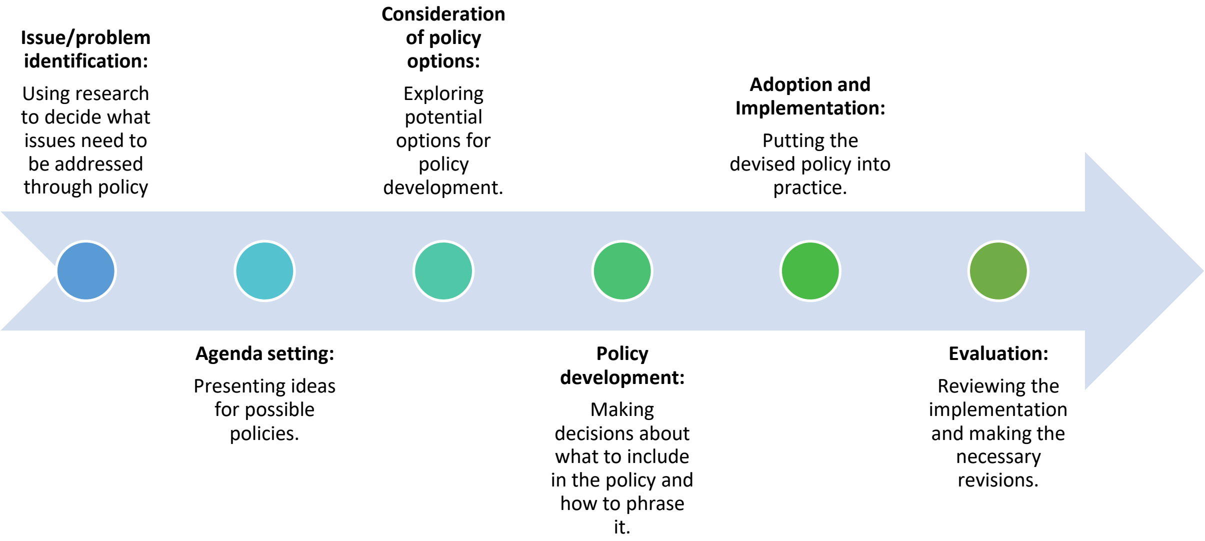
5.2 Policy development

If you have determined that none of these policies exist in your country, use the stakeholder analysis you created in the previous section to determine which of those stakeholders identified would be best placed to develop relevant policies.

Stakeholders can be:

- experts in online safety issues who can contribute to the subject matter, and
- individuals who understand legislative procedures who can contribute essential information towards policy development.

It is also good to identify who needs to be part of the policy development process and eventual implementation to ensure that the process is not stalled. The policy development process is outlined in Figure 10.



Issue/problem identification: Using research to decide what issues need to be addressed through policy

Agenda setting: Presenting ideas for possible policies.

Consideration of policy options: Exploring potential options for policy development.

Policy development: Making decisions about what to include in the policy and how to phrase it.

Adoption and Implementation: Putting the devised policy into practice.

Evaluation: Reviewing the implementation and making the necessary revisions.

Figure 11: Policy development process

Once you have identified the relevant stakeholders who can help draft and develop the policy, it is useful to locate any existing model policies or similar policies. These can save you time, and point you in the right direction.

To help you out, below is a list of some existing resources:

- The 5Rights Foundation Child Online Safety Toolkit provides a practical and accessible guide for online safety policy development, international best practices and a model child online safety policy.
- The International Telecommunication Union Child Online Protection (COP) Guidelines for policy-makers present a user-friendly flexible framework that can be adopted by governments and policy-makers to help develop effective child protection on a national level. (Apart from guidelines for policy-makers, the ITU has also published guidelines for children, parents/carers, educators, and industry).
- The CO:RE Policy Directory is a searchable database that contains the relevant actors, organisations and policies in the field of policy-making for children, youth and digital technologies in Europe.
- Apart from model policies, the following are other useful resources for developing policies and legislation:
- Australia's Online Safety Act 2021, some of the strongest legislation in the world, which sets about establishing an eSafety Commissioner, Australia's independent regulator for online safety.
- The WeProtect Model National Response helps countries and organisations respond to child sexual exploitation and abuse within their contexts.
- The International Centre for Missing and Exploited Children CSAM Model Legislation and Global Review (currently in its 9th edition), analyzes CSAM legislation from around the world and presents various aspects to consider in drafting anti-CSAM legislation.
- The International Centre for Missing and Exploited Children Online Grooming of Children for Sexual Purposes Model Legislation and Global Review analyzes legislation from around the world that focus on online grooming of children for sexual purposes. It also includes definitions, offenses, sanctions, sentencing, regional and international laws, implementation and good practices.
- The African Union initiative on Strengthening Regional and National Capacity and Action against Online Child Sexual Exploitation and Abuse in Africa is a continental plan for the years 2020-2025 to accelerate actions related to the prevention, protection and prosecution of OCSEA.

Other documents to consider include:

- The United Nations Convention on the Rights of the Child established in 1989 is broadly ratified and the subsequent General Comment No. 25 from 2021 focuses on how these rights apply in the digital environment. These are important documents to consider when advocating for online safety policies to be developed. Moreover, the UN has developed additional protocols such as the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, which supplement the convention on specific issues. The Concluding Observations of the Committee on the Rights of the Child indicate the progress achieved by the reviewed State in relation to the implementation of the Convention on the Rights of the Child, main areas of concern and recommendations for improvement. This can also be useful to review issues related to online safety and to use as an advocacy document.
- The United Nations Sustainable Development Goals, as child online safety is relevant to attaining several of these goals, particularly when issues intersect (see Module 7.

5.3 Policy implementation and reinforcement

A proper policy implementation is achieved when those responsible for the policy engage in specific activities to ensure that it is reaching its targets. When assessing the existing policies, you might have identified some policies that exist already, but that need to be revised, updated, implemented or enforced. In order to lobby efficiently for these changes to be made, it is advisable to understand and specify the changes needed clearly.

Answer the following questions in relation to these policies and based on your answers, you will identify how best to target these changes through your advocacy strategy.

- When was the policy devised?
- Have there been any recent revisions to the policy?
- Which issues have become relevant to this policy but are not included in it?
- Are the goals of this policy sufficiently clear?
- To what extent are the intended outcomes of the policy being achieved?
- Who is responsible for implementing and monitoring this policy?
- Is there adequate resourcing dedicated to achieving policy outcomes?
- What are the barriers for this policy to be properly implemented?
- What needs to be done to remove these barriers?
- Who are the stakeholders that need to be involved in order to remove these barriers?
- Are there any cooperation or coordination mechanisms that need to be developed to address these issues?

Module 6: Advocacy tactics

In this module, you will find some tactics you can apply in your advocacy strategy. Once you learn more about these tactics, you can identify the best tactic to deliver your key message to specific stakeholders.

Adequate communication strategies are essential to advocacy. The following principles are useful reminders to ensure your advocacy message comes across clearly, coherently and credibly[15]:

- be succinct and clear;
- pay careful attention to who delivers the message;
- avoid exaggeration;
- be aware of negative stereotypes’
- do not put the activists at risk of any form of harm, and
- protect the dignity, safety and privacy of the beneficiaries of the advocacy strategy.

When it comes to advocating for online safety, it is also important to remember to:

- keep in mind child safeguarding principles throughout,
- avoid feeding media panics[2] about online risks, and
- ensure you have access to the latest high-quality data or evidence.

ChildFund Alliance members have already been applying some of the advocacy tactics that are presented here within their online safety programs (Figure 12). This module will present further information about these tactics, so you can develop and expand your advocacy repertoire. It will also present some examples of how ChildFund Alliance members have been applying these advocacy tactics.

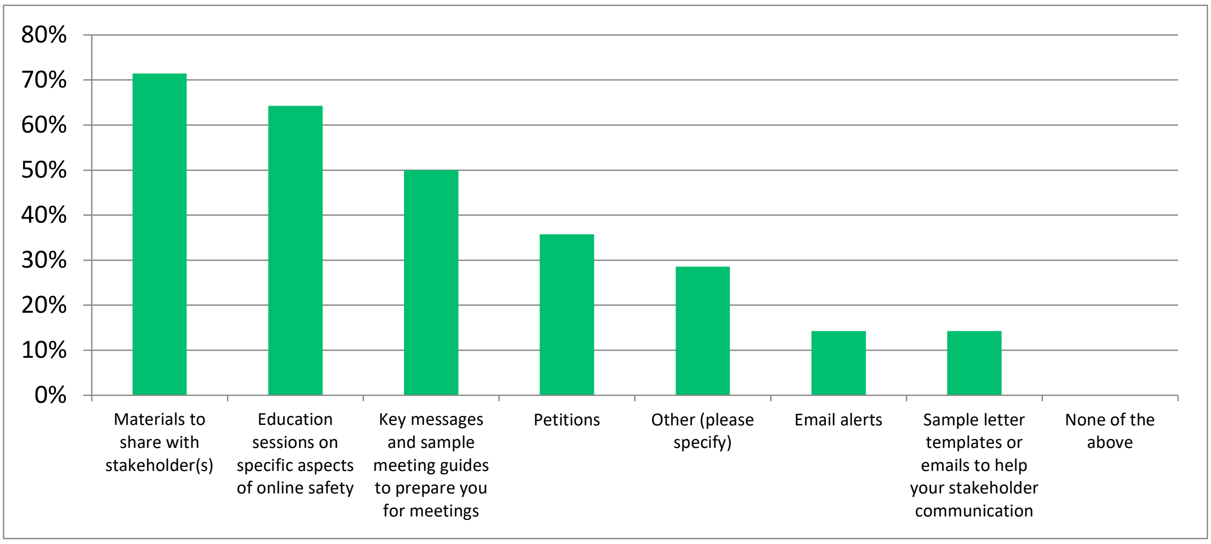


Figure 12: Advocacy tools applied in online safety programs

[2] Media panic happens when media try to instil fear in adults about the dangers of new tech and online risks for children. This happens through appealing to emotions, over sensationalising the issues, exaggerating or through selective reporting.

6.1 Campaigning

Campaigns are a series of strategic and planned activities that take place over a period to achieve a set of objectives. These activities are usually targeted towards the stakeholders you have identified.

Campaigning can serve the following purposes in relation to your online safety advocacy strategy by:

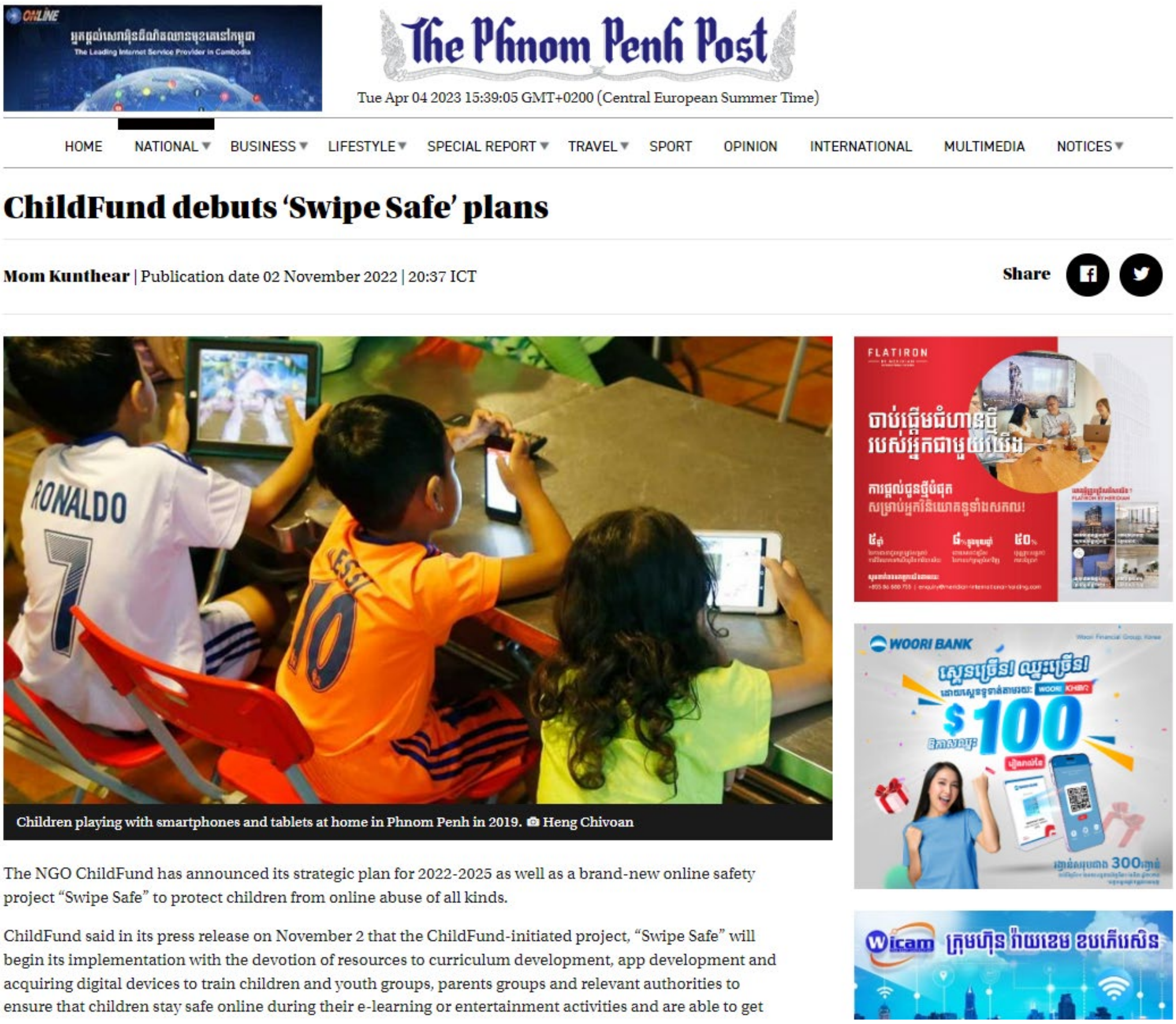
- establishing the importance of addressing online safety issues,
- raising awareness and educating the general public and specific target groups (e.g., children, parents or carers, educators, etc…) about online safety issues,
- increasing pressure on policy-makers and decision-makers to develop and implement adequate policies and legislation for child protection in the online environment,
- Generating debate about online safety issues in public fora, the media, etc,
- increasing public support for online safety issues,
- educating the public about the importance of online safety issues, and
- developing support and partnerships for your organisation.

Some ways in which campaigning can be carried out are presented below[16,17,18]. Aspects, such as establishing partnerships, are explained in other sections of this module. Usually, you would use a combination of some of these tactics within a campaign that spans over an established period. Such tactics can be used on their own or within a campaign, and it is ideal to have several methods that contribute to disseminating your main messages as widely as possible.

Swipe Safe is a campaign (Figure 13) organised by ChildFund Cambodia aiming to help children navigate their online lives safely, and to support parents and child protection professionals through strengthening their knowledge and skills about online child abuse. The campaign has the following four outcomes targeting various stakeholders:

1. Government and duty bearers are supported to equip frontline child protection, law enforcement and justice officers to tackle and respond to online child sexual exploitation and abuse.
2. Diverse groups of children and young people are empowered to actively adopt stronger online self-protective behaviours.
3. Parents and caregivers are equipped with knowledge, skills and behaviors to enable them to be online safety partners for children and young people, preventing and responding to online risks and harms.
4. Sharing evidence and advocating for integrating Swipe Safe modules into existing national systems.

A key outcome of the Swipe Safe Campaign is the putting forward one voice to support the government in implementing a national action plan to prevent and respond to Online Child Sexual Exploitation (OCSE), since there is currently no specific law against OCSE. Another key outcome is the recognition of the Swipe Safe Curriculum by the government's Cambodia National Council for Children (CNCC). The campaign was also reported in the news to increase the visibility of its aims.



ChildFund debuts 'Swipe Safe' plans

Mom Kunthear | Publication date 02 November 2022 | 20:37 ICT

Children playing with smartphones and tablets at home in Phnom Penh in 2019. Heng Chivoan

The NGO ChildFund has announced its strategic plan for 2022-2025 as well as a brand-new online safety project "Swipe Safe" to protect children from online abuse of all kinds.

ChildFund said in its press release on November 2 that the ChildFund-initiated project, "Swipe Safe" will begin its implementation with the devotion of resources to curriculum development, app development and acquiring digital devices to train children and youth groups, parents groups and relevant authorities to ensure that children stay safe online during their e-learning or entertainment activities and are able to get

Figure 13: News coverage of the Swipe Safe Campaign launch

Using traditional and new media: This is explained in more detail in section 6.2.

Carrying out an online campaign: If you have decided to carry out a campaign, it is important to back it with an online campaign. Here you will use web-based tools to sustain and disseminate information about your campaign, communicate what is happening in your campaign, advertise, etc. An online campaign is relatively easy to set up and can give you wider reach and help you gather support for your online safety cause. It is generally cheap and provides you with data about those who are getting involved with your channels.

If you choose to carry out an online campaign, keep in mind the following:[16]

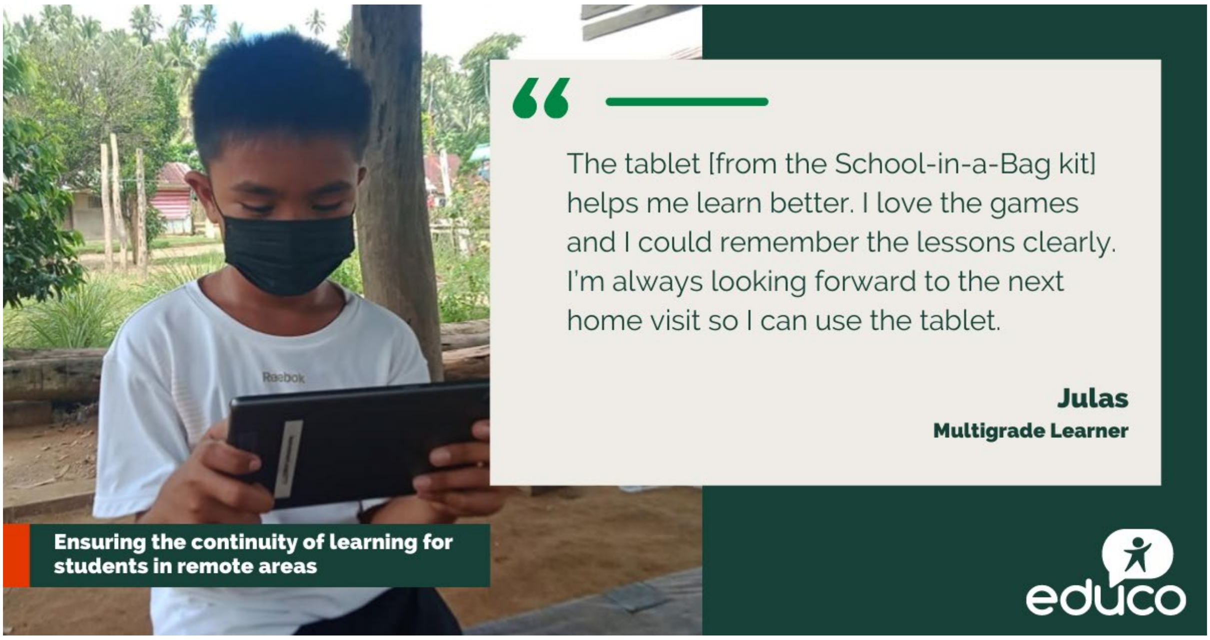
- The principles of communicating about online safety issues presented in this module.
- Ensure that you have planned your online campaign well.
- Learn about your target audiences; that group(s) you are seeking to influence. For example, in the context of a national advocacy strategy related to online safety, if you are seeking policy and legislative change, your target audience will likely be the government.
- Use multiple social media channels but ensure you are directing people to a single online source (usually a website) which holds all information relating to your campaign
- Make your content simple yet engaging so that it attracts your audiences' attention and increases the likelihood that the content is shared.
- Play by the 'rules' of the different channels. Know when to use which kind of content, e.g., images, videos, hashtags, tagging, and more.
- Ensure that your online campaign is consistent with your offline campaign.
- Engage in live conversations with your followers.

Disseminating pamphlets, flyers, posters, and resources: Printed media can be an effective way to communicate your key messages to your target audiences. Posters and flyers are printed visual aids that present your key message in a straightforward way, using visuals, a slogan and some key information. Pamphlets are similar but they enable you to present more information. These materials can be distributed everywhere throughout your campaign. They can be useful for schools, waiting rooms or other places where people will be waiting for a service, and for any of the other campaigning events being discussed in this module.

If you have the resources available, you might also want to create some useful free items (for example, laptop webcam covers), that you can distribute with your key message. This can get your audience to think about online safety issues, like why they should cover their laptop camera. Other materials that can be disseminated include resources, toolkits, and learning materials, among others.

In the Philippines, Educo has a collaborative relationship with UNICEF to help bring hope to young learners in difficult areas. Through the Learning Recovery Program of Children in Multigrade Schools of Southern Leyte and Dinagat Islands project, schools hit by Typhoon Rolly are assisted in learning recovery.

School-in-a-Bag and Learning Passports are resources distributed to identified schools. These are digital resources for teachers and students to hasten the learning recovery of these typhoon-hit schools where children's educational needs have been severely affected. Although this is not a strictly online safety program of Educo, it involves the use of tablets and other education technologies by teachers (and their students). One of the learning materials provided to the schools is the e-Citizenship package, which contains presentations and guidelines on OCSEA-related topics.



"The tablet [from the School-in-a-Bag kit] helps me learn better. I love the games and I could remember the lessons clearly. I'm always looking forward to the next home visit so I can use the tablet.

Julas
Multigrade Learner

Ensuring the continuity of learning for students in remote areas
educo

Figure 14: Educo Philippines Facebook post promoting the School-in-a-Bag resources

Conducting talks, workshops and presentations: Identify existing opportunities where you can present your work and online safety issues to your stakeholders. One example is to establish collaborative partnerships with schools. You might not be able to visit every school in your country to discuss the importance of online safety, but you can create hybrid events where schools can participate online and continue discussing the topics you introduce. If these opportunities do not exist, you might decide to create your own around specific events happening in your context or internationally (e.g., Safer Internet Day or World Children's Day)

Participating in conferences, public meetings and fora: Through these opportunities where there are people gathered to discuss relevant issues, you can put forward your case for increasing online safety awareness and action. You can also organise these events yourself. You can invite your stakeholders, the community, and anyone who is interested can contribute to the discussion.

Using mailing lists: If you have a mailing list that your followers have signed up for, you can disseminate any campaign material. Make sure you are following the terms and conditions that subscribers agree to when they sign up to be part of this list.

Conducting surveys and opinion polls: The public can be asked questions about the key messages you are advocating for to examine any changes in attitudes or sentiments towards online safety issues. You can publish these results and potentially use them to gain media coverage of your campaign.

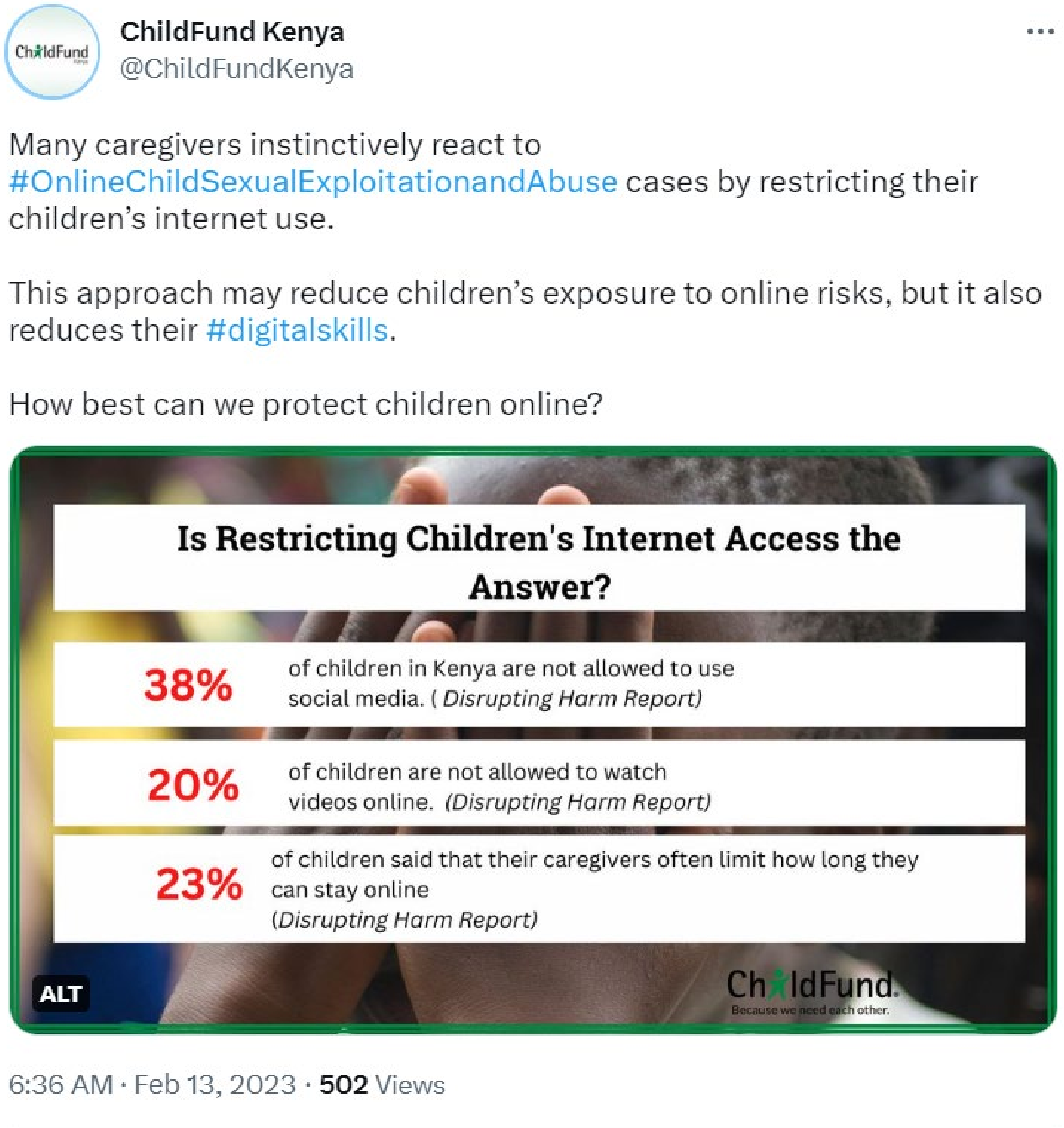
Performances and stunts: These could be creative and fun ways to engage your audiences. Artistic performances can be thought-provoking and include the participation of children and young people to present their voice and perspective on online safety issues. Stunts, on the other hand, can be good for media coverage but might require more resources.

Public stalls: Your organisation can be present in person at public events through a stall where you can showcase the work you do, give information about the need for advocacy in the field of child online safety, distribute any information you have available (e.g., pamphlets or flyers) and ask people to take action (e.g., by signing a petition). Ensure you have an approachable, attractive and reachable approach to having a public stall for maximum effectiveness.

Organise a petition: Through a petition, you can ask people to sign their name in support of a specific issue that you need decision-makers to take action on in relation to your online safety advocacy strategy. Petitions are then presented to the relevant decision-makers. Using a petition shows that you have public support for your issue and this can increase pressure on them to act in favour of the issue you are pushing. This can be the introduction of a new policy or a proper implementation of an existing policy. There are many online tools you can use to get people to sign and share the petition. Look into these tools if you decide to use this advocacy tactic, and make sure that you provide concise information on your advocacy issue and why people should sign.

Organising rallies, marches or demonstrations: These involve gathering your supporters and marching in support for your cause. They increase the visibility of your issue and show that the issues you are advocating for have widespread support. Make sure you plan these events well, obtaining the necessary permits, ensure the safety of marchers and consider inviting the press if it is safe to do so.

As part of their campaign, ChildFund Kenya was able to advocate for online safety on their social media platforms like Facebook, LinkedIn and Twitter (Figure 13). This was also done on the mainstream media through TV and radio interviews.



ChildFund Kenya
@ChildFundKenya

Many caregivers instinctively react to #OnlineChildSexualExploitationandAbuse cases by restricting their children's internet use.

This approach may reduce children's exposure to online risks, but it also reduces their #digitalskills.

How best can we protect children online?

Is Restricting Children's Internet Access the Answer?

38% of children in Kenya are not allowed to use social media. (*Disrupting Harm Report)*

20% of children are not allowed to watch videos online. *(Disrupting Harm Report)*

23% of children said that their caregivers often limit how long they can stay online *(Disrupting Harm Report)*

6:36 AM · Feb 13, 2023 · 502 Views

Figure 15: ChildFund Kenya campaign Twitter post

An important part of the campaign was the procession walk, which was conducted on Safer Internet Day in Kilifi County. This coastal county is rampant with sex-tourism and online sexual exploitation of children and so the march was carried out here, with high participation from children and young people (Figure 15 and Figure 16).

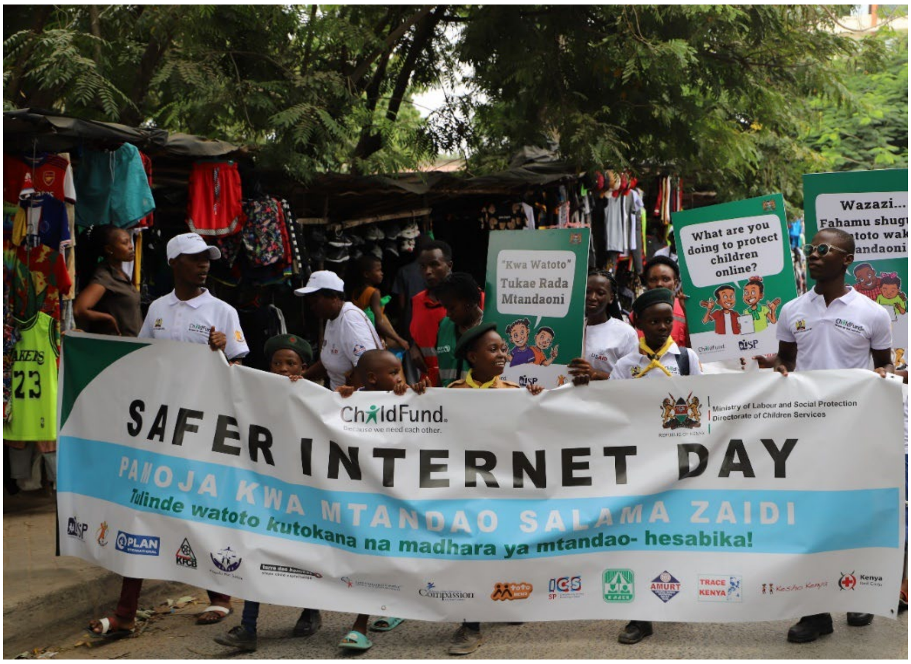

SAFER INTERNET DAY
PAMOJA KWA MTANDAO SALAMA ZAIDI
Tulinde watoto kutokana na madhara ya mtandao- hesabika!
ChildFund
Ministry of Labour and Social Protection
Directorate of Children Services
"Kwa Watoto" Tukae Rada Mtandaoni
What are you doing to protect children online?

Figure 16: Children lead the Safer Internet Day Advocacy Walk in Kilifi Kenya.

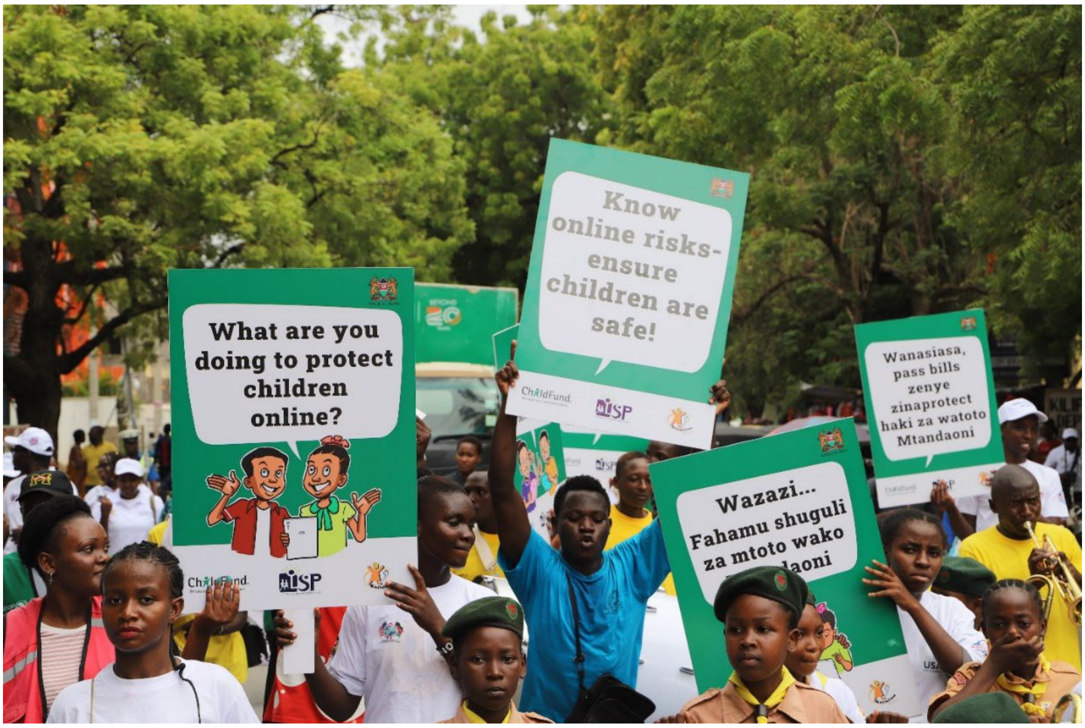

What are you doing to protect children online?
Know online risks- ensure children are safe!
Wanasiasa, pass bills zenye zinaprotect haki za watoto Mtandaoni
Wazazi... Fahamu shuguli za mtoto wako

Figure 17: Promoting different messages to stakeholders during the Safer Internet Day Procession in Kilifi Kenya

Disseminating success stories: Consider the possibility of disseminating the success stories where advocacy efforts in other countries have achieved the goals expected.

6.2 Using media and social media

Media is crucial to advocacy. Using the various channels available through print, broadcasting and electronic media, you can convey information about online safety and the issues associated with it to various stakeholders. This increases the issues' visibility, disseminates the correct information, increases awareness and shapes public perceptions about online safety.

The principles of communication outlined at the beginning of this module are important to engaging with the media. Often you might find yourself facing a situation where what is considered newsworthy by the media is not the message about online safety issues that you want to promote.

Make sure your message has news value, ensure it is relevant, interesting, and visually appealing. Do not be tempted to twist your message into something that the media will pick up as this undermines the integrity of your advocacy strategy. It is also counterproductive given that you will be addressing the subject of online safety through your communications.

Both old and new forms of media can be useful to your online safety advocacy strategy. It is ideal to use a mix as this increases the chances of reaching your target audiences. Here are some ways in which you can engage with different forms of media:

Participating in TV and radio discussions and giving interviews: These are opportunities to get your message across to specific audiences through a live or recorded segment. These are some tips[15,16] you can use to prepare yourself and to engage in media participation:

- Do some background research on the journalist, interviewer and their company.
- Determine who their target audience is.
- If possible, ask for the questions you will be asked beforehand.
- If you are not able to receive the questions beforehand, anticipate what questions you might be asked. Include potentially difficult questions.
- Practice how you want to answer these questions.
- Know what you want to say.
- Know what you do not want to say.
- Prepare how you want to phrase your message.
- Make your message simple and straightforward.
- Prepare a 'soundbite' – a memorable phrase that summarises your core message.
- Know the most important pieces of evidence that will support your message (e.g., some statistics, data about online safety issues that are relevant to the discussion) and the source of this evidence.
- Practice segueing from answering any question you are asked to your core message.
- Keep calm and do not get too emotional or flustered.
- Always be polite. You can be passionate and authentic but generally, anger is counterproductive.
- Present your key message as soon as possible in the interview or discussion.
- Conclude the interview by repeating your key message once again.

As part of their online safety program, Children Believe Ethiopia collaborated with FM Radio 107.8 to develop a series of radio messages on OCSEA. These were broadcast nationwide with the aim of providing the population with useful, practical and relevant information to help in the prevention of online harm against children.

The serial radio messages consist of seven episodes that were broadcast on seven consecutive working days from October 24 to November 1, 2022 focusing on:

1. the results of their research on Online Child Abuse and Exploitation (OCSEA) in Ethiopia,
2. the types of OCSEA,
3. children's access to pornographic videos and the law,
4. hacking and theft of children's social media passwords,
5. blackmailing of children through online platforms,
6. sexual extortion of children, and
7. online grooming of children for sexual purposes.

The radio messages included the real stories and experiences of children with OCSEA, ways of identifying, reporting and responding to child online safety risks and suspected OCSEA, as well as discussion of the relevant international and national laws on the topic.

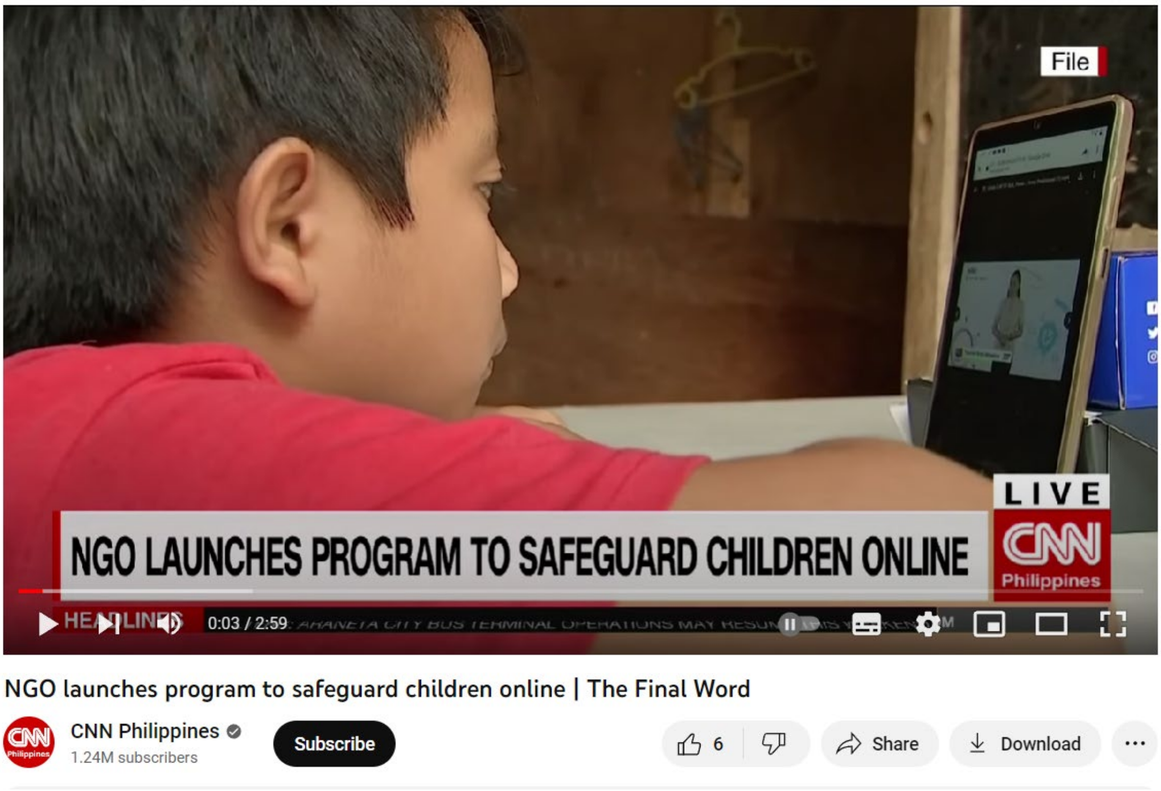
These messages also focused on the roles and responsibilities of governmental and non-governmental actors, parents, caregivers, children, and the community as a whole in strengthening OCSEA prevention and response mechanisms. Lawyers, information technology experts, and CB-Ethiopia staff were involved in the development and recording of the messages.

Figure 18: Recording of the serial radio messages on OCSEA by Children Believe Ethiopia

Publishing features and photos spreads: Presenting your news stories in creative formats that can attract the readers' attention. Using visuals such as infographics and photos makes your article or feature more appealing.

Writing letters to the editor or opinion pieces: Get your message in the media by addressing the editor in a letter or contributing an opinion piece (op-ed) where you share your opinion about the online safety issues concerned.

Establishing working relationships and engaging with journalists: Journalists decide the kind of exposure your issues will receive in the media, so it is important to establish and build relationships with journalists to keep them updated about developments in the field of child online safety. ChildFund Philippines has been promoting their campaign using the media to increase awareness of the campaign and the issues it addresses. The [feature in the CNN Philippines] (Figure 13) is one such example. Apart from being featured on TV, the campaign was also covered on online news portals such as [Minda News], [Palawan News] and [Amianan Balita Ngayon].


NGO launches program to safeguard children online | The Final Word

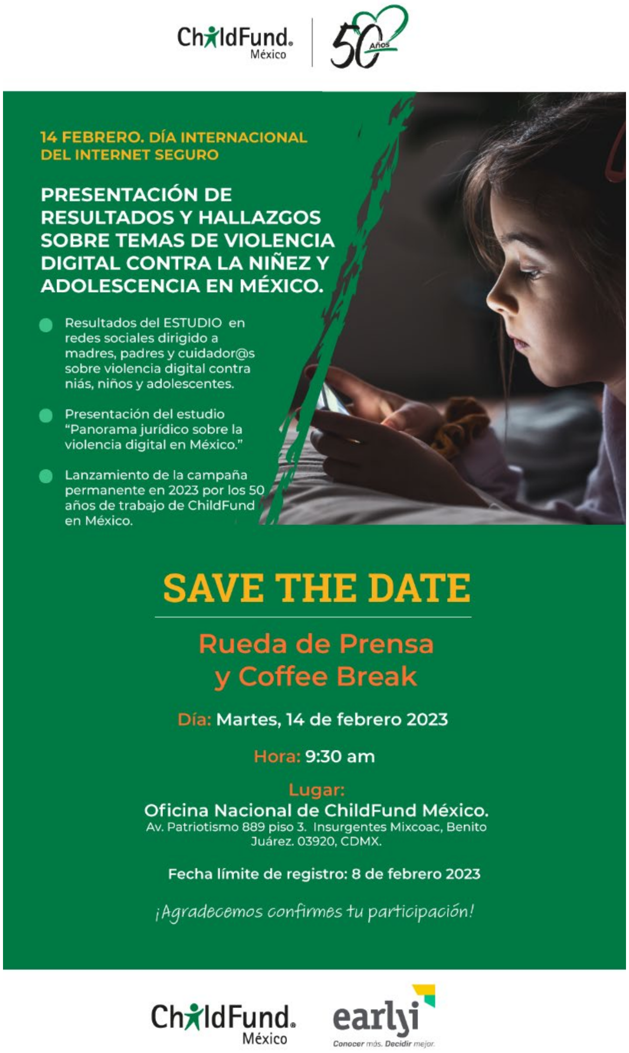
CNN Philippines
1.24M subscribers

Figure 19: CNN Philippines reporting on ChildFund's Online Safety Program

Writing press releases: These are announcements published by your organisation which keep the public and journalists informed about events, recent developments related to child protection online, publications, etc. Press releases should be written clearly and concisely, and the essential information should be conveyed in the first few paragraphs. Apart from being published on your own channels, press releases are also sent to journalists and news organisations so that they are disseminated with their audiences.

Organising a press conference: Press conferences are events to which media are invited. You can use press conferences to make important announcements, launch a campaign, or present key research findings. Media reporters are given the opportunity to ask questions or interview key individuals. They use the material generated from the press conference to write and publish a news story. Holding a press conference involves preparation and planning[19], including the preparation of key messages, organisational logistics, and a press kit that is usually distributed to the media attending the event.

ChildFund Mexico organised a press conference (Figure 19) on Safer Internet Day to present the results and findings from their work themed around digital violence against children and young people. The press conference had a significant impact. Over 20 media outlets (Figure 20) published or presented the information related to Online Sexual Exploitation and Abuse of Children shared during the press conference on their portals.



ChildFund. México | 50 Años

14 FEBRERO. DÍA INTERNACIONAL DEL INTERNET SEGURO

PRESENTACIÓN DE RESULTADOS Y HALLAZGOS SOBRE TEMAS DE VIOLENCIA DIGITAL CONTRA LA NIÑEZ Y ADOLESCENCIA EN MÉXICO.

- Resultados del ESTUDIO en redes sociales dirigido a madres, padres y cuidador@s sobre violencia digital contra niás, niños y adolescentes.
- Presentación del estudio "Panorama jurídico sobre la violencia digital en México."
- Lanzamiento de la campaña permanente en 2023 por los 50 años de trabajo de ChildFund en México.

SAVE THE DATE

Rueda de Prensa y Coffee Break

Día: Martes, 14 de febrero 2023

Hora: 9:30 am

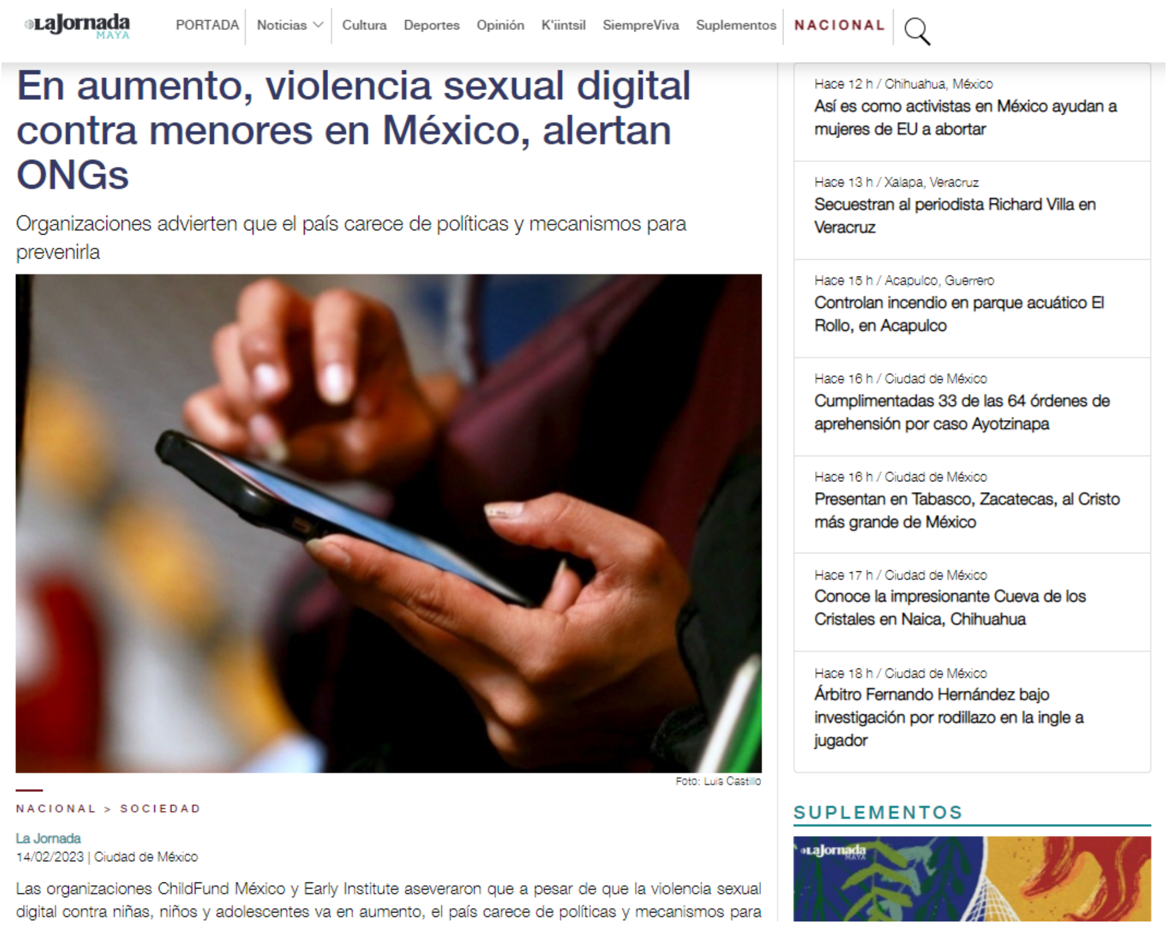
Lugar:
Oficina Nacional de ChildFund México.
Av. Patriotismo 889 piso 3. Insurgentes Mixcoac, Benito Juárez. 03920, CDMX.

Fecha límite de registro: 8 de febrero 2023

¡Agradecemos confirmes tu participación!

ChildFund. México | early Conocer más. Decidir mejor.

Figure 20: Flyer announcing the ChildFund Mexico Press Conference



En aumento, violencia sexual digital contra menores en México, alertan ONGs

Organizaciones advierten que el país carece de políticas y mecanismos para prevenirla

Foto: Luis Castillo

NACIONAL > SOCIEDAD

La Jornada
14/02/2023 | Ciudad de México

Las organizaciones ChildFund México y Early Institute aseveraron que a pesar de que la violencia sexual digital contra niñas, niños y adolescentes va en aumento, el país carece de políticas y mecanismos para

Hace 12 h / Chihuahua, México
Así es como activistas en México ayudan a mujeres de EU a abortar

Hace 13 h / Xalapa, Veracruz
Secuestran al periodista Richard Villa en Veracruz

Hace 15 h / Acapulco, Guerrero
Controlan incendio en parque acuático El Rollo, en Acapulco

Hace 16 h / Ciudad de México
Cumplimentadas 33 de las 64 órdenes de aprehensión por caso Ayotzinapa

Hace 16 h / Ciudad de México
Presentan en Tabasco, Zacatecas, al Cristo más grande de México

Hace 17 h / Ciudad de México
Conoce la impresionante Cueva de los Cristales en Naica, Chihuahua

Hace 18 h / Ciudad de México
Árbitro Fernando Hernández bajo investigación por rodillazo en la ingle a jugador

SUPLEMENTOS

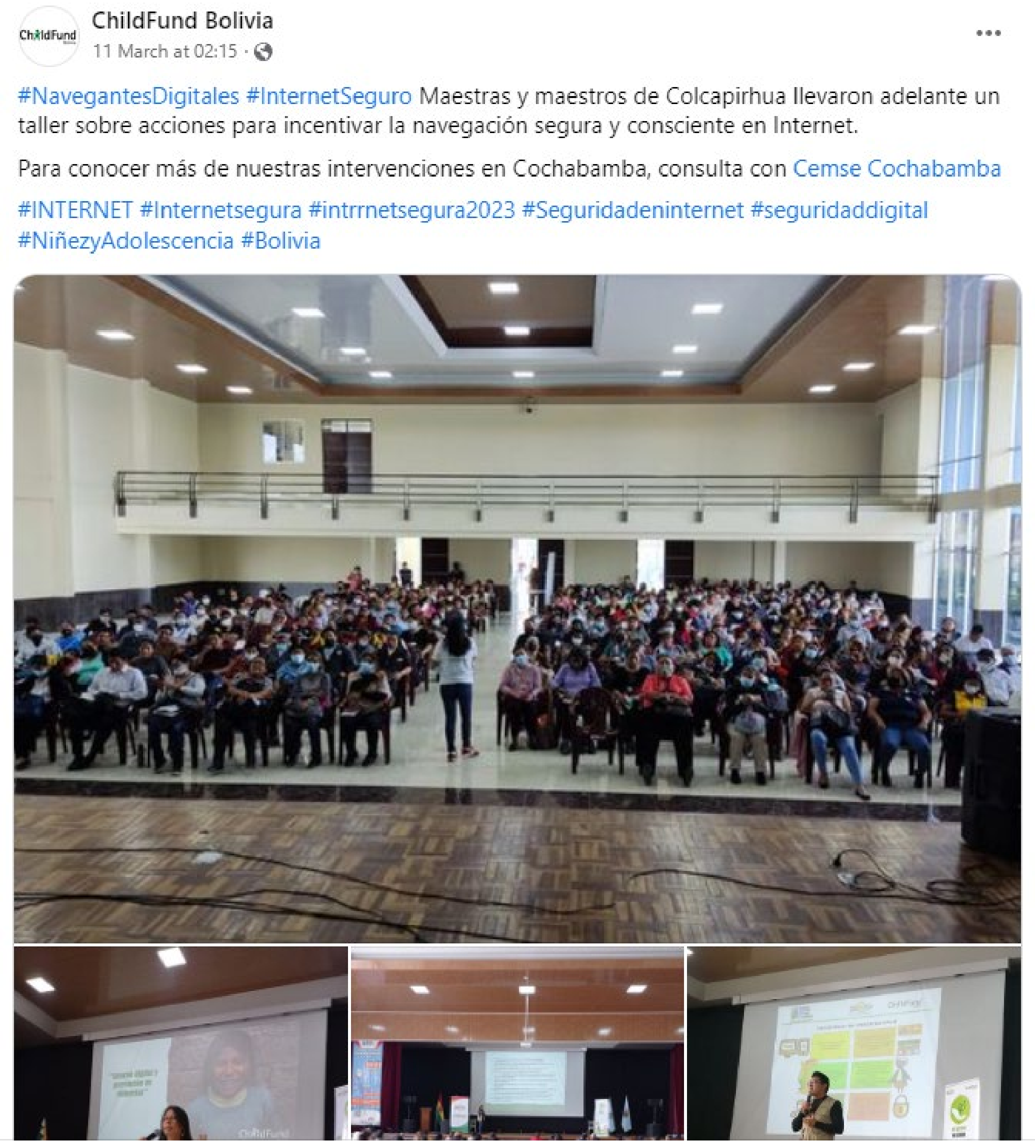
Figure 21: News coverage following ChildFund Mexico's press conference

Having an online presence: An online presence is an accessible and easy way to promote your key messages. This can include having an updated website, regular blogs and newsletters, and using your social media profiles. The latter are widely used (although there might be some country-specific restrictions) but generally, you can post content on your channels to share them with your followers. You can also use these channels to share new blogposts, updates and your newsletter. It is important to have your audience engage with your posts, but this should be treated with caution. Follow your social media channels and ensure that you contribute to timely comments, particularly if there are comments on your posts that challenge your key advocacy messages.

ChildFund Bolivia is engaged in an online safety program focused on the prevention of online sexual exploitation and abuse of children. The program has four key actions:

1. Design with the participation of children and adolescents the content of the tools and strategies for the prevention of sexual violence online.
2. Intergenerational work between children, adolescents, parents, and teachers to achieve a protective digital accompaniment.
3. Involve schools in training children, adolescents, and teachers to prevent online sexual violence.
4. Mass media campaigns to raise awareness about OSEAC.

As part of their program, they work in schools to strengthen the digital literacy of children, adolescents, parents, and teachers. In this way, not only can children navigate safely but their parents and teachers can also provide support through positive communication. The Navegantes Digitales campaign activities are well-documented on the social media profile of ChildFund Bolivia, with frequent posts and visuals, which are always accompanied by the hashtag #NavegantesDigitales.



ChildFund Bolivia
11 March at 02:15 ·

#NavegantesDigitales #InternetSeguro Maestras y maestros de Colcapirhua llevaron adelante un taller sobre acciones para incentivar la navegación segura y consciente en Internet.

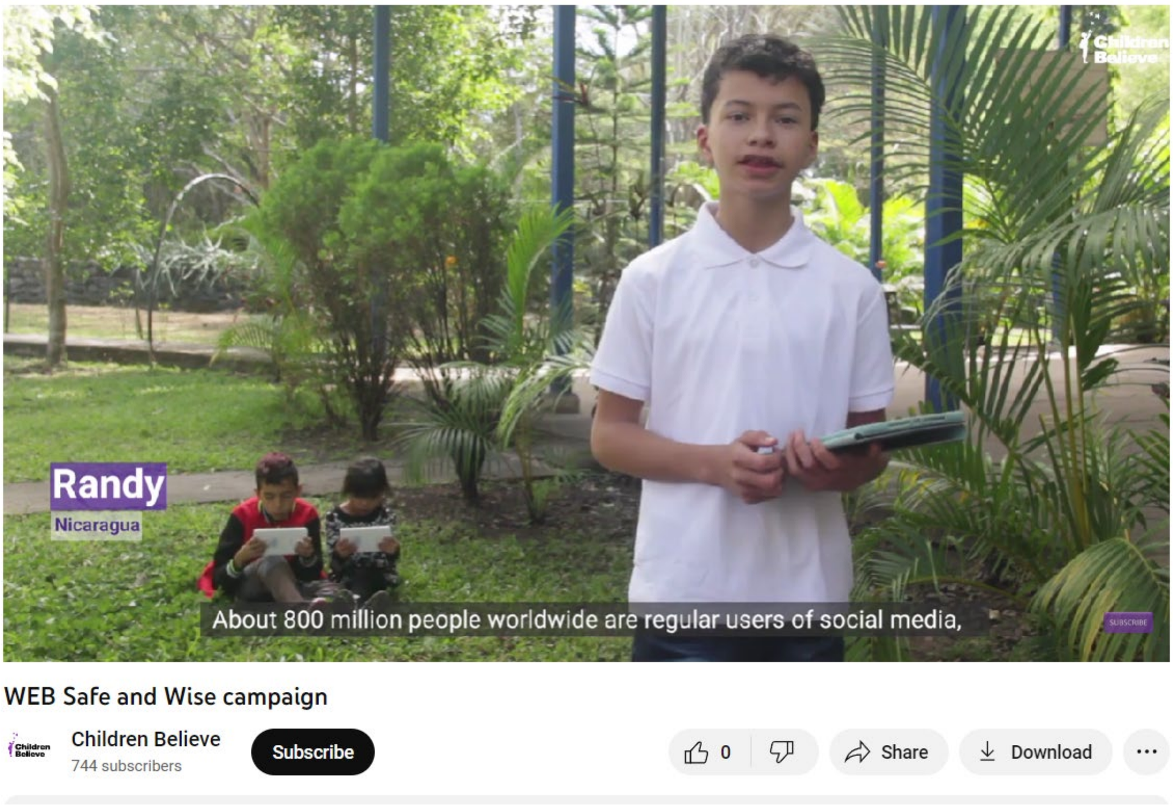
Para conocer más de nuestras intervenciones en Cochabamba, consulta con Cemse Cochabamba

#INTERNET #Internetsegura #intrrnetsegura2023 #Seguridadeninternet #seguridaddigital #NiñezyAdolescencia #Bolivia

Figure 22: ChildFund Bolivia social media post to promote the #NavegantesDigitales Campaign

Publishing videos: As part of your strategy, you may also decide to use brief videos that present your key messages. Professionally produced videos are more appealing but, understandably, you might not have sufficient resources to commission these. However, one option could be to collaborate with an institution providing training in media production and engaging an intern to work on such productions at a reduced fee.

Children Believe in Nicaragua has produced a video (Figure 18) as part of the WEB Safe and Wise Campaign to promote children and adolescents' safe use of digital tools. In this video, children and young people raise awareness about issues affecting them online, such as online child sexual abuse, cyberbullying, the need for education, and the lack of regulation and legislation.



About 800 million people worldwide are regular users of social media,

WEB Safe and Wise campaign

Children Believe
744 subscribers

Figure 23 - Screenshot of the Video Produced by Children Believe

Sharing personal testimonies: In the area of online safety advocacy, personal testimonies can be a powerful way to show how the lack of online safety has influenced the lives of children and young people. Such stories give a human touch to your core messages. Yet, you need to be careful how to present such testimonies to ensure the safety, dignity, privacy and ideally anonymity of the children giving their testimony and that they do not experience re-traumatisation from sharing their experiences.

6.3 Lobbying and negotiating

Lobbying is the process of convincing stakeholders who are influential or able to make decisions to take specific actions in line with your online safety advocacy strategy. Some of these actions can be policy analysis, policy development or policy implementation. Module 5 has already presented some strategies and resources which you can apply in this field. Other strategies through which lobbying can be carried out are presented below.

Meetings with officials, policy-makers or decision-makers: These meetings are an opportunity to present online safety issues to individuals who have the most power to influence and act in support of these issues. Such meetings can result in strategic alliances and working relationships with people in power, and help you achieve your online safety advocacy goals. Plan and prepare for these meetings well. These are some tips[16] to consider:

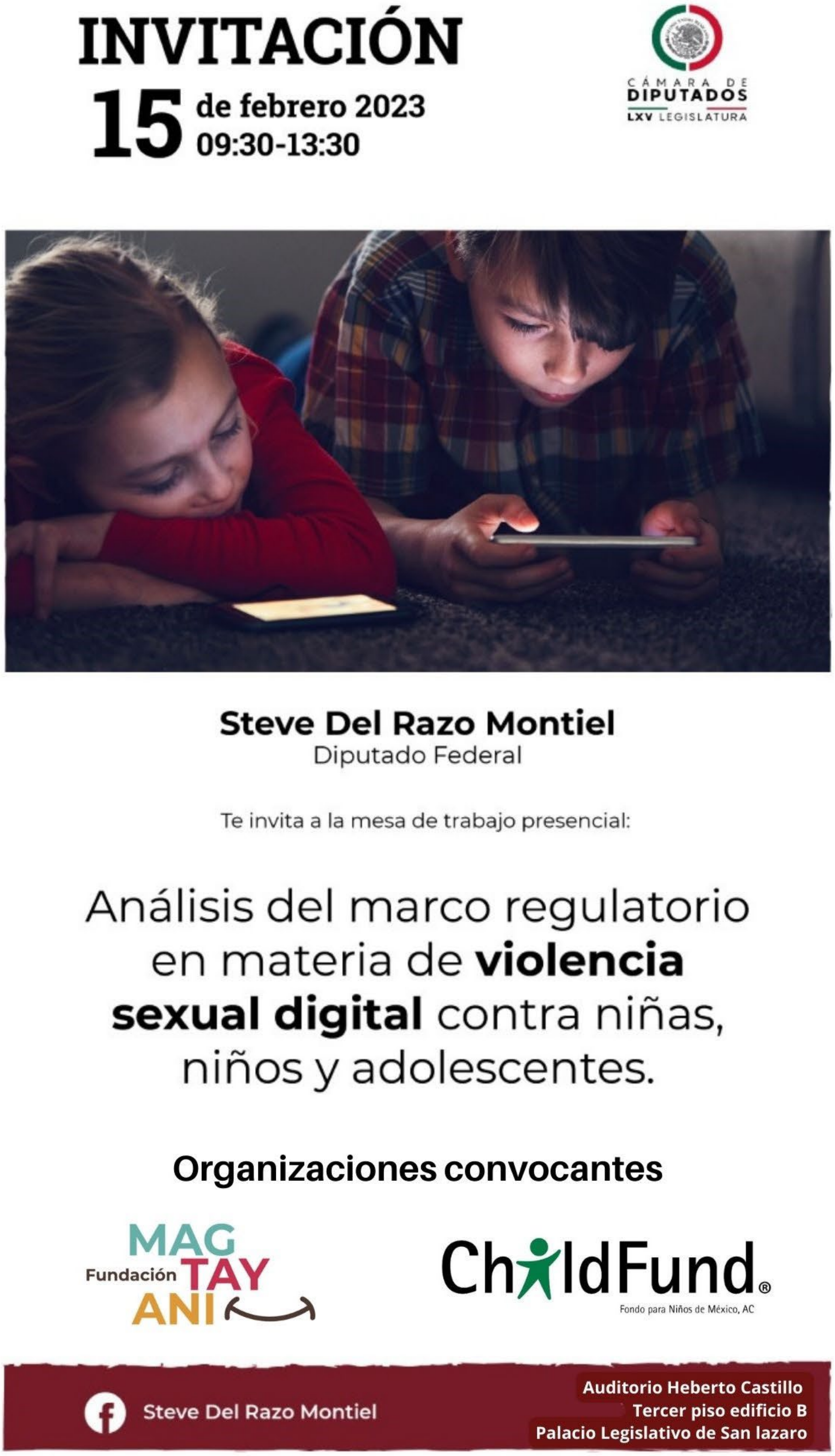
- Assess if this is the right timing to be making specific requests.
- Be clear about your aims and what you are asking from them.
- Try to figure out what their position on online safety issues is.
- Identify who could be the best people to attend this meeting.
- Ensure you have prepared the key message you want to get across.
- Ensure that you have sufficient evidence to back your claims.
- Prepare a brief presentation to highlight your key message.
- Have a plan B in case something unexpected happens in your meeting.
- Anticipate possible responses, objections and questions and prepare yourself to discuss these.

During the meeting, it is important to keep an open mind. Communicate your key messages clearly but also listen and acknowledge what the policy-makers say. Engage in dialogue and try to focus on common ground rather than disagreements. At times, you will find that you need to help officials develop a position about child online safety if these issues are not on their agenda. Try to reach a conclusion where courses of action are agreed.

After each meeting, take some notes to help you remember which individuals were present for the meeting, the issues discussed, their understanding and level of alignment with your goals, the kind of influence they have, and any actions they committed to pursue. This information is important to be able to engage in timely and relevant follow-ups to your meetings.

ChildFund Kenya is currently working on engaging parliamentarians to allocate resources to online child protection agencies to help them respond to OCSEA issues across Kenya. In Bolivia, through the successful interventions of Educo, the Attorney General's Office is one-step away from assuming the responsibility of addressing the alerts issued by NCMEC (National Center for Missing and Exploited Children) in terms of alerts of possible cases of online sexual exploitation of children.

There is also a move towards presenting a proposal for the criminalization of child online sexual exploitation within the framework of the modification of Law 263 Against Human Trafficking. In Mexico, ChildFund is also engaging policy-makers. They are currently preparing an initiative to present to Congress that address problems in the Federal Penal Code, and they invited the public for a discussion with a policy-maker about regulations related to digital sexual violence against children and young people (Figure 22).



INVITACIÓN

15 de febrero 2023
09:30-13:30

CÁMARA DE DIPUTADOS
LXV LEGISLATURA

Steve Del Razo Montiel
Diputado Federal

Te invita a la mesa de trabajo presencial:

Análisis del marco regulatorio en materia de **violencia sexual digital** contra niñas, niños y adolescentes.

Organizaciones convocantes

Fundación MAG TAY ANI

ChildFund
Fondo para Niños de México, AC

Steve Del Razo Montiel

Auditorio Heberto Castillo
Tercer piso edificio B
Palacio Legislativo de San lazaro

Figure 24: Invitation Flyer for a local politician for ChildFund Mexico's Discussing Digital Violence Against Children event

If it is very difficult to meet officials, another way to lobby can be to write letters or emails to elected officials, policy-makers or decision-makers. These letters can be used to give information, to explain the salience of online safety issues for children, to ask for support and to make specific propositions, among others. If you establish that letter writing is the best way to reach these individuals, this guide can help you prepare your letters.

Negotiating: This is a form of persuasion used when there are different views or positions between relevant parties and an agreement needs to be reached. Each side will have stakes in obtaining the best way forward for them. If you identify that such a tactic is necessary to reach your advocacy aims, prepare beforehand not to be caught off guard or discover that you gave up more than you were willing to.

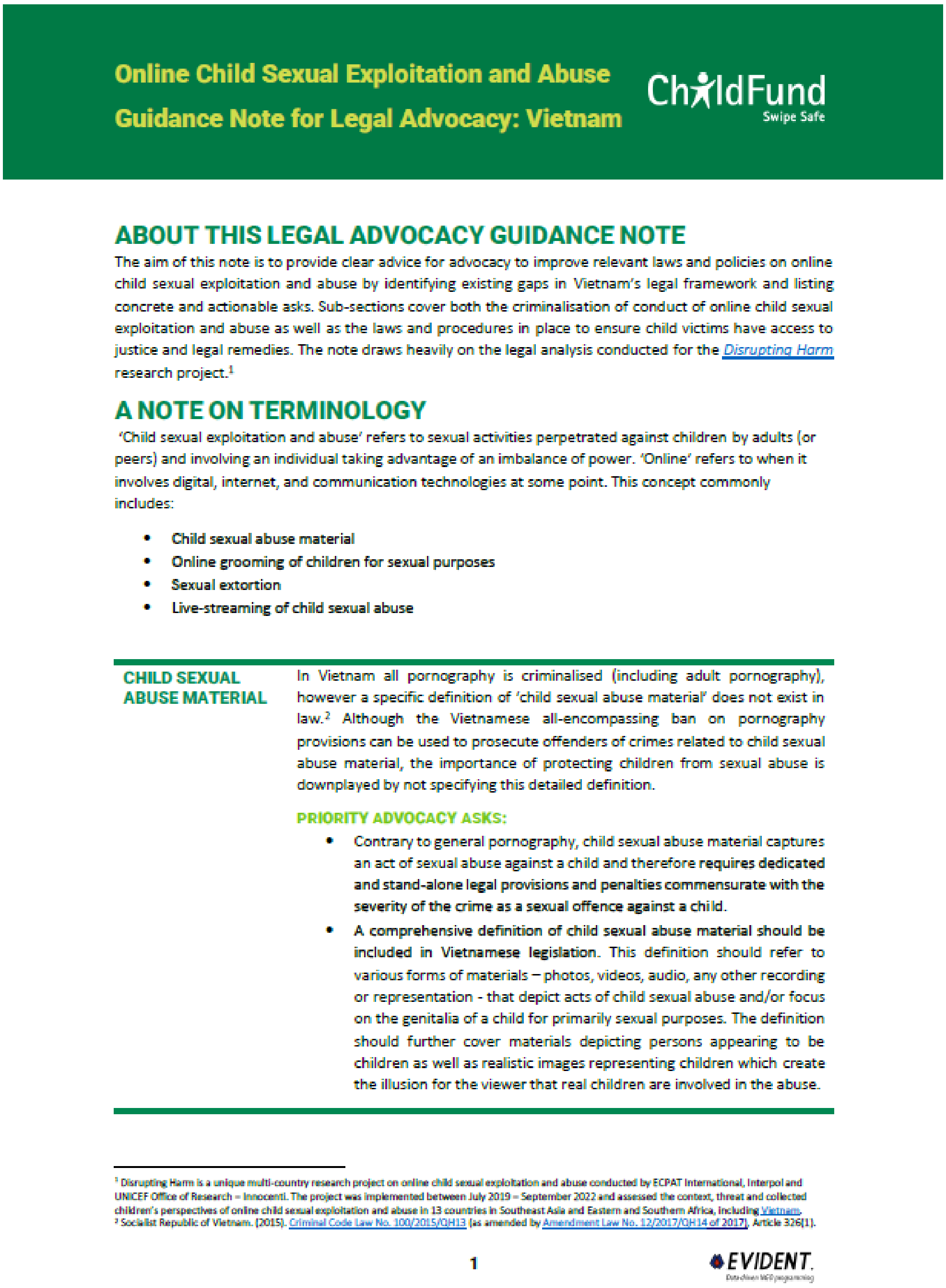
These are some tips[16] to consider:

- What do you wish/need to obtain?
- What is the minimum achievement you would be comfortable with?
- What is the other party expecting to gain?
- Can you offer anything that they want?
- Which concessions would you be willing to make?
- Drive a hard bargain; do not make concessions easily.
- It is better to aim a bit higher and then negotiate down.
- Can your asks be broken down into smaller components?
- Focus on your shared ground to help you work out agreements.

Legal action: This is a more advanced form of lobbying and it is not always ideal to opt for such action. As a last resort, lawsuits, legal litigation and civil actions can be part of your advocacy strategy if other strategies have failed to achieve the desired results. Before engaging in such strategies, it is advisable to ensure that you and your organisation have the adequate legal background and backing to be able to do so and have considered the potential risks involved. Another advocacy tactic related to legislative frameworks is to highlight gaps in policies and legislation and contribute to their development.

Since 2022, ChildFund Vietnam has been working with child protection systems to strengthen the capacity of frontline staff, law enforcement and government agencies, to protect girls and boys from online violence. One of the specific objectives is to establish a National Coordination Mechanism to strengthen the holistic prevention, response and support for online child protection issues.

ChildFund Vietnam has also developed a legal advocacy online safety guide (Figure 23) to improve relevant laws and policies on online child sexual exploitation and abuse by identifying existing gaps in Vietnam's legal framework and listing concrete and actionable asks in relation to child sexual abuse material, online grooming, live-streaming of child sexual abuse and access to justice for child victims of online sexual exploitation and abuse.



Online Child Sexual Exploitation and Abuse
Guidance Note for Legal Advocacy: Vietnam

ChildFund Swipe Safe

ABOUT THIS LEGAL ADVOCACY GUIDANCE NOTE

The aim of this note is to provide clear advice for advocacy to improve relevant laws and policies on online child sexual exploitation and abuse by identifying existing gaps in Vietnam's legal framework and listing concrete and actionable asks. Sub-sections cover both the criminalisation of conduct of online child sexual exploitation and abuse as well as the laws and procedures in place to ensure child victims have access to justice and legal remedies. The note draws heavily on the legal analysis conducted for the *Disrupting Harm* research project.[1]

A NOTE ON TERMINOLOGY

'Child sexual exploitation and abuse' refers to sexual activities perpetrated against children by adults (or peers) and involving an individual taking advantage of an imbalance of power. 'Online' refers to when it involves digital, internet, and communication technologies at some point. This concept commonly includes:

- Child sexual abuse material
- Online grooming of children for sexual purposes
- Sexual extortion
- Live-streaming of child sexual abuse

CHILD SEXUAL ABUSE MATERIAL

In Vietnam all pornography is criminalised (including adult pornography), however a specific definition of 'child sexual abuse material' does not exist in law.[2] Although the Vietnamese all-encompassing ban on pornography provisions can be used to prosecute offenders of crimes related to child sexual abuse material, the importance of protecting children from sexual abuse is downplayed by not specifying this detailed definition.

PRIORITY ADVOCACY ASKS:

- Contrary to general pornography, child sexual abuse material captures an act of sexual abuse against a child and therefore **requires dedicated and stand-alone legal provisions and penalties commensurate with the severity of the crime as a sexual offence against a child.**
- **A comprehensive definition of child sexual abuse material should be included in Vietnamese legislation.** This definition should refer to various forms of materials – photos, videos, audio, any other recording or representation - that depict acts of child sexual abuse and/or focus on the genitalia of a child for primarily sexual purposes. The definition should further cover materials depicting persons appearing to be children as well as realistic images representing children which create the illusion for the viewer that real children are involved in the abuse.

[1] Disrupting Harm is a unique multi-country research project on online child sexual exploitation and abuse conducted by ECPAT International, Interpol and UNICEF Office of Research – Innocenti. The project was implemented between July 2019 – September 2022 and assessed the context, threat and collected children's perspectives of online child sexual exploitation and abuse in 13 countries in Southeast Asia and Eastern and Southern Africa, including Vietnam.
[2] Socialist Republic of Vietnam. (2015). Criminal Code Law No. 100/2015/QH13 (as amended by Amendment Law No. 12/2017/QH14 of 2017), Article 326(1).

Figure 25: ChildFund Vietnam Legal Advocacy Guidance Note

ChildFund Ecuador's Naveguemos Seguros (Let us navigate Safe) initiative aims to influence different levels of the state, society and families to contribute to a framework for the protection of children and adolescents against violence in the digital world, especially sexual violence. The initiative has five main pillars, one of which relates to the regulatory framework. This work involves guaranteeing the digital rights of children and adolescents through creating a legal framework that guarantees these rights. Together with 21 public and private institutions, ChildFund Ecuador devised the public policy for a safe internet for children and adolescents. ChildFund also sent its own contributions to the National Assembly about the digital rights of children and adolescents for the proposed reform of the Comprehensive Organic Code of Children and Adolescents, and about online sex crimes against children and adolescents for the reform of the Comprehensive Organic Criminal Code. A key outcome of the Naveguemos Seguros initiative is the collaboration with the Ministry of Education in the development of the protocols that ensure sustainability within the institution to influence and ensure the quality of its contents, in addition to fighting for the continuity of its dissemination and consolidation in future budgets of the institution.

This alliance with the Ministry also allows the protocols to have a national and multi-year scope and potentially reach the entire educational system. In a second stage, ChildFund Ecuador will develop educational communication products to enhance the reach and understanding of the protocols.

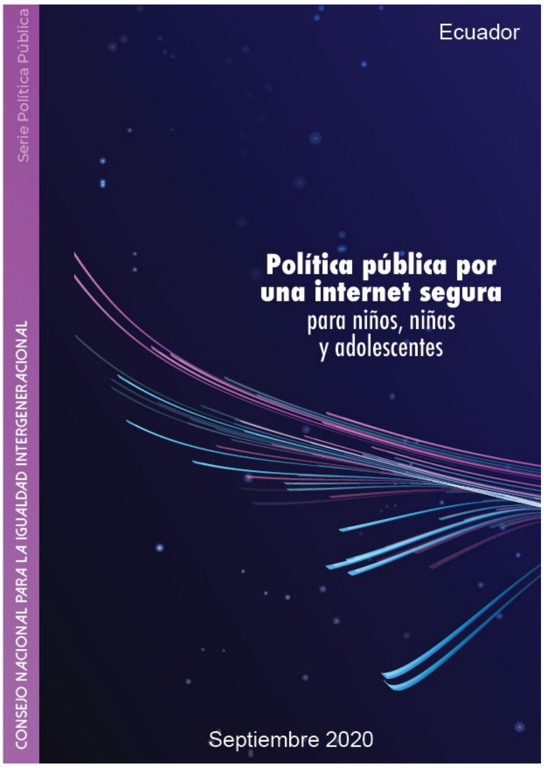

Serie Política Pública
CONSEJO NACIONAL PARA LA IGUALDAD INTERGENERACIONAL
Ecuador
Política pública por una internet segura para niños, niñas y adolescentes
Septiembre 2020

Figure 26: Public Policy for a Safer Internet for Children and Adolescents developed by ChildFund Ecuador

6.4 Establishing partnerships

Partnerships involve bringing together people, groups or organisations that have similar aims or are already working in the field of child online safety. Such partnerships can be both an outcome of your advocacy strategy or interim goals with your advocacy strategy to help you reach larger overarching goals. Partnerships can be short or long-term. The advantages include combining strengths, networks, resources, and knowledge among the partners. Partnerships also increase credibility, avoid duplicating work, and ensure that the resources available are used effectively. Moreover, such allegiances can have greater influence when advocating for online safety issues as policy-makers find it difficult not to 'hear' your messages. Working towards a common goal with others is also more motivating and provides a space to support each other.

The following are some ways in which you can develop your networks and establish partnerships:

Networking: Introducing yourself and the work you do as an organisation in the relevant spaces is important to networking. It also involves talking to people you already have contacts with about your online safety advocacy cause. Your network may have further connections with people or organisations who are interested in your cause or working in a similar field. Ask to be introduced to these people or organisations when possible. This increases your network and ensures your campaign has a wider reach.

Joining networks: Being a part of specific networks working in the field of online safety and child protection can give you access to information, resources, training opportunities, and important contacts in the field.

Reaching out to potential collaborators: Creating opportunities where people can come together and they can learn about your work, you can learn about theirs, and explore potential synergies.

Forming alliances and coalitions: Identifying organisations who share the same vision and establishing partnerships with them. Generally, such partnerships have a clear, shared purpose and an established structure or system through which to advocate for child safety online.
One example is happening in Kenya. ChildFund is supporting the development of the National OCSEA manual for social service providers that will be used to build their response to OCSEA issues in Kenya (Figure 14). Through the online program, ChildFund is also developing Standard Operating Procedures and guidelines for interagency coordination to help social service providers to offer effective and coordinated services to the survivors of OCSEA in the county (Figure 15).

Figure 27: Participants during the development of the National OCSEA manual for social service providers

Figure 28: A representative from Plan International presenting the development of SOPs

Establishing research partnerships: Collaborating with research institutes, universities and higher education institutions will help you identify existing research, research gaps in the child online safety arena in your context and develop new research. You can also apply for research grants together or create mutual relationships where students carry our research projects in collaboration with your organisation.

During 2020, Educo Bolivia collaborated with other organisations to carry out two research studies focusing on the recruitment of children and young people for commercial sexual violence and sexual exploitation on social media and the deep web. The report *Sistematización de dos Investigaciones Referidas a la Captación y Offerta de Violencia Sexual Commercial en Redes Sociales e Internet Profunda* (Figure 29) summarises the results from these two studies and presents the most relevant findings analyzed from a sociological and gender perspective.

The report applies an intersectional perspective (see Module 7) to understand the networks of power linked to gender, class and ethnicity, which are behind the industry and the sex market. The report details recruitment strategies, such as false job offers, phishing, online entrapment and pharming, used by adults to induce young people to generate sexual content. The report also explores the difficulties victims face in recognising this as violence and in exiting these situations, together with the issues related to the pervasiveness of such material online and how it effects the recovery, healing and the social reintegration of victims.

SISTEMATIZACIÓN
DE DOS INVESTIGACIONES REFERIDAS A LA
CAPTACIÓN Y OFERTA DE
VIOLENCIA SEXUAL COMERCIAL
EN REDES SOCIALES E INTERNET PROFUNDA

Figure 29: Research Report on Commercial Sexual Violence by Educo Bolivia

Establishing thematic partnerships: Partnering with your local Safer Internet Centre, the Online Safety Helpline or the local CSAM reporting hotline also enables you to gain access to strategic information related to child online safety. This increases your awareness of issues that need to be addressed and your advocacy strategy can be backed by timely and relevant data from these sources. These organisations usually belong to networks such as Better Internet for Kids, Insafe and INHOPE among others. These organisations can also be gateways to important information and resources.

Establishing 'unlikely' partnerships: Your online safety advocacy cause can be also supported by partners who might not be directly involved in this field, but wish to help promote your key messages. For example, hospitals and healthcare centres may agree to have posters in patient waiting rooms. Public transport companies may be able to provide free advertising on buses or at waiting stations. Partnerships can also be established with organisations working in a different or loosely related field. Such unlikely partnerships can still contribute to your advocacy strategy and help you increase your influence.

6.5 Engaging and mobilising the community

Part of your advocacy strategy could include ways in which you tap into the strengths, energies and resources of the community. Online safety issues for children can only be addressed when the responsibility for child protection online is shared among various stakeholders. The community can be an important stakeholder in this process. As awareness about online safety increases and the community feels more empowered to take action, the issue of online safety achieves a higher position on the agenda, and pressure on decision-makers is likely to increase.

You have already identified who the relevant stakeholders in the community are and what key messages you want to put forward to them. Within these communities, you are likely to find different levels of involvement; some will be able to take more active or leadership roles. Apart from using advocacy tactics to mobilise your community (presented in the section about campaigning) here are some other ways in which you can reach your community to increase their engagement in online safety advocacy:

Informal community meetings: Participating in meetings such as community group meetings, town meetings, religious and cultural events where you can engage with these groups and inform them about online safety issues.

Invitations for involvement: Inviting community members to join the cause and support the work directly, either by volunteering or doing any other work that serves the online safety advocacy cause.

ChildFund Philippines has a child and youth-led advocacy project in Cagayan de Oro to combat OCSEA. The project aims to increase awareness on the issue of OCSEA and create a local plan of action and policies so that children become more responsive to child protection issues. Cagayan de Oro is a hot-spot community affected by OCSEA and the project is hoping to address children's vulnerability to OCSEA, increase parents' awareness, and tackle the lack of programs and policies on OCSEA.

After the preparation and the baseline assessment period, the program trained young people to become OCSEA warriors or change agents. These 22 OCSEA warriors are recognized youth leaders and they continue to spread the learnings from the program across their communities, to increase awareness of about online safety within the community. In addition to establishing these 22 OCSEA warriors, the program has reached 70 youth leaders and over 20,000 individual children and family members. A series of child-led roundtable meetings and opportunities for dialogue were also held, to influence the local government, parents and caregivers (Figure 30), and a launch of the campaign was held to generate awareness of the program.

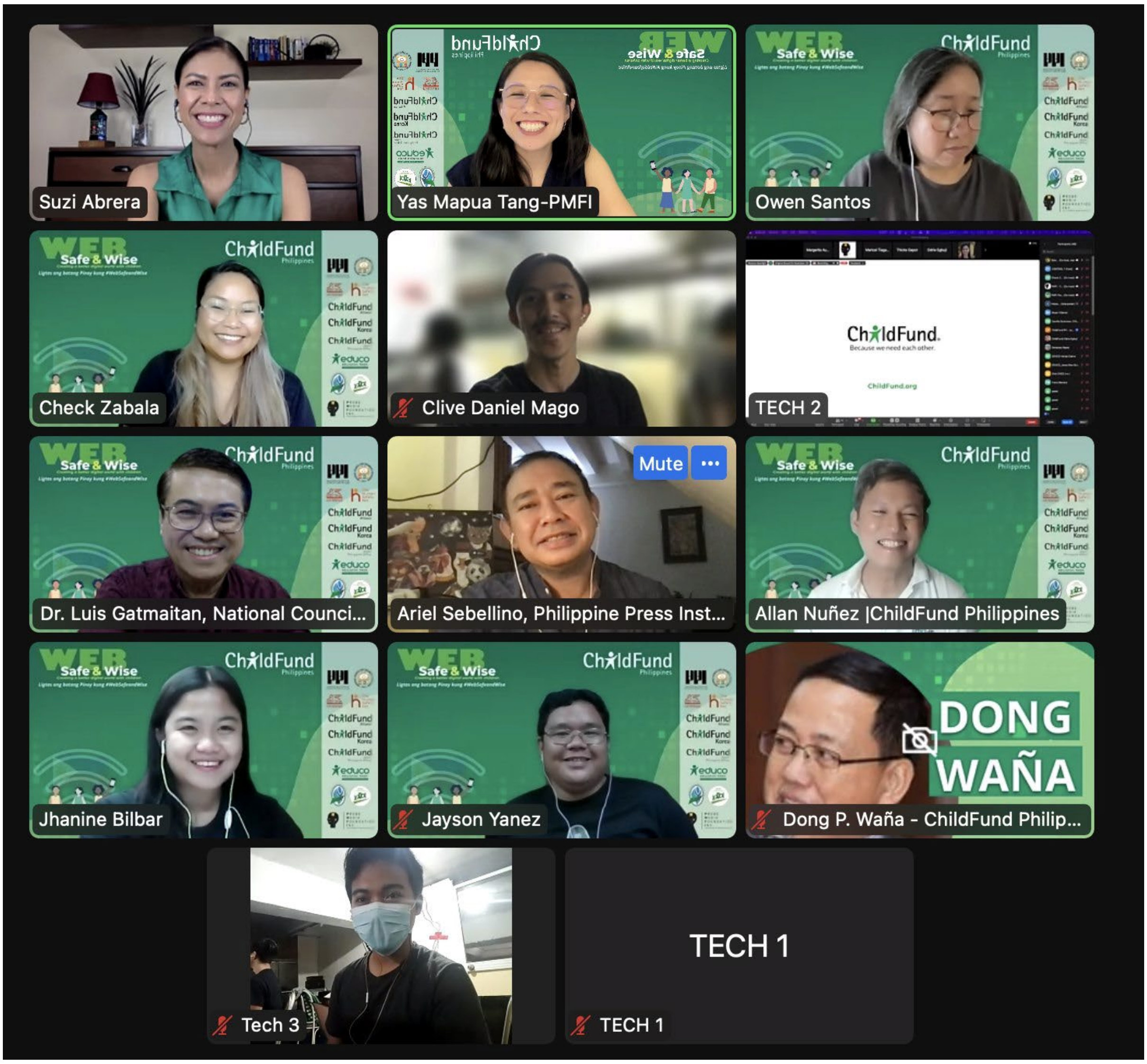
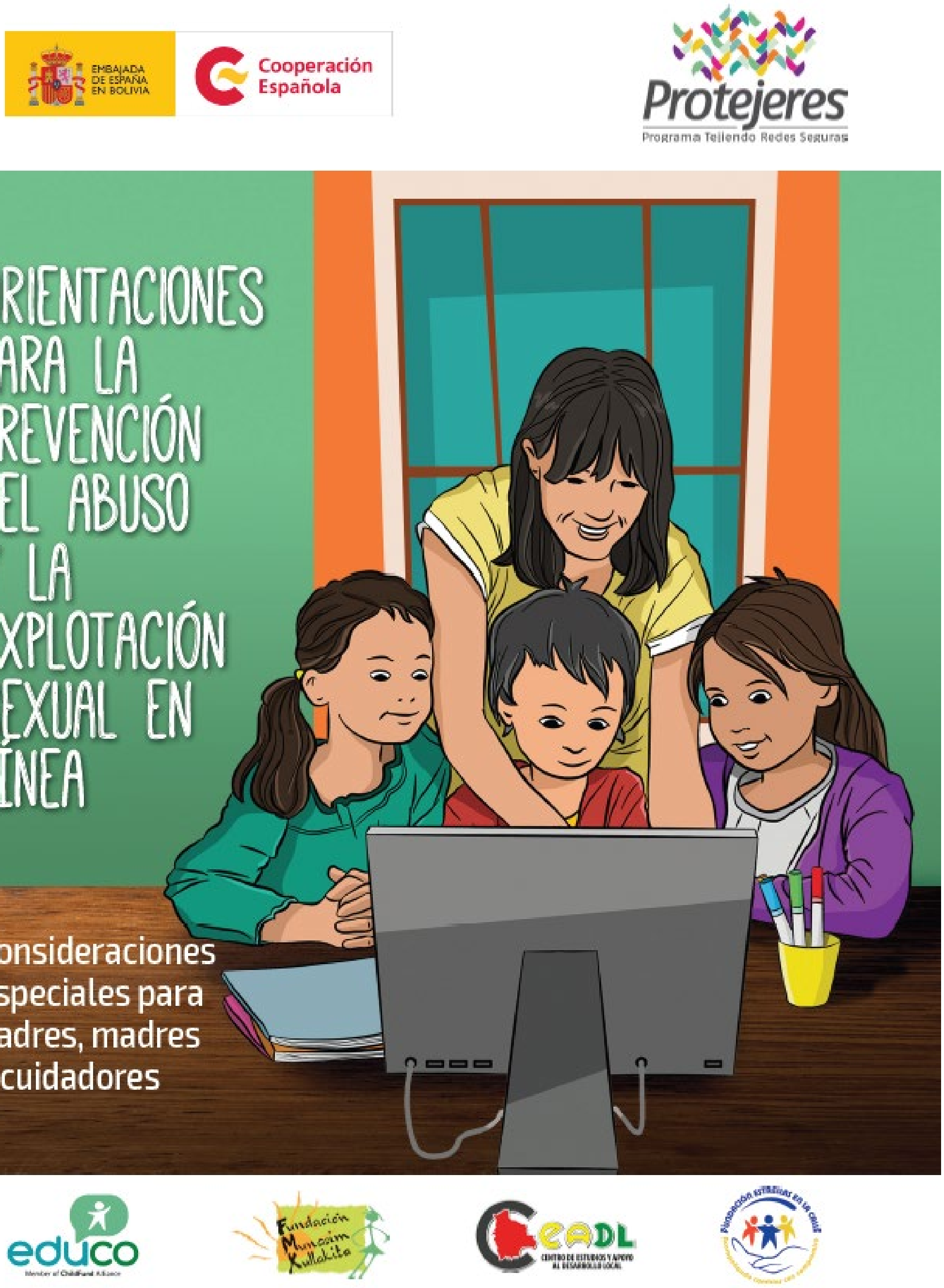

Suzi Abrera
Yas Mapua Tang-PMFI
Owen Santos
Check Zabala
Clive Daniel Mago
ChildFund.
TECH 2
Dr. Luis Gatmaitan, National Counci...
Mute
Ariel Sebellino, Philippine Press Inst...
Allan Nuñez |ChildFund Philippines
Jhanine Bilbar
Jayson Yanez
DONG WAÑA
Dong P. Waña - ChildFund Philip...
Tech 3
TECH 1
TECH 1

Figure 30: One of ChildFund Philippines online roundtable discussions

Working with community leaders: Establishing connections with trusted community leaders who have a gatekeeper role within some communities, can eventually give you access to the community.

Collaborating with cause champions or influencers: Identifying high profile or influential individuals who engage with the public through their own strategies and channels, who can promote online safety issues. Ensure you select influencers wisely so that the messages they share are coherent and consistent with your campaign.

Organising communities: Carrying out work within communities to empower them to engage in further advocacy. One example of this is the PROTEJERES (Programa Tejiendo Redes Seguras) program by Educo Bolivia, which contributes to the fight against human trafficking for commercial sexual exploitation purposes and related crime. In addition to the advocacy component, they promote the creation of digital communities, as children, adolescents and youth own spaces in which they can share, talk, discuss, propose and build. While the project targeted both children and governmental bodies, parents, the community, public school teachers and the private sector (represented by hotels, motels, travel agencies, the media and carriers) were also among the main targets of the program. The publication *Orientaciones para la prevención del abuso y la explotación sexual en línea. Consideraciones especiales para padres, madres y cuidadores* (Figure 31) provides information about prevention from online sexual abuse to mothers, fathers and caregivers.



ORIENTACIONES PARA LA PREVENCIÓN DEL ABUSO Y LA EXPLOTACIÓN SEXUAL EN LÍNEA

Consideraciones especiales para padres, madres y cuidadores

EMBAJADA DE ESPAÑA EN BOLIVIA
Cooperación Española
Protejeres
Programa Tejiendo Redes Seguras
educo
Member of ChildFund Alliance
Fundación Munasim Kullakita
CEADL
CENTRO DE ESTUDIOS Y APOYO AL DESARROLLO LOCAL

Figure 31: Orientaciones para la Prevención del Abuso y la Explotación Sexual en Línea published by Educo Bolivia.

6.6 Choosing the right tactics to deliver key messages to your stakeholders

Which tactics you choose for your advocacy strategy will depend on several factors. The following factors are some aspects to consider when making your choice:

- Is there a tactic that clearly fits the key message that you want to pass on to your identified stakeholders?
- Which tactic best fits the kind of change are you aiming to achieve?
- What skills or expertise do you have at your disposal?
- What technical resources do you have available?
- What financial resources do you have available?
- What human resources do you have available?
- How can you leverage your network?
- Can this tactic help you achieve your advocacy strategy goals?

In Module 2, we addressed three different types of change: awareness, will, and action. In Module 4, we identified three different types of stakeholders: public, influencers and decision-makers. Coffman and Beer (2015)[7] illustrate how the specific nature of change and the type of stakeholders require a variety of advocacy tactics. This is represented in Figure 11 below and it can help you choose the right tactics depending on your audiences and the types of change achievable.

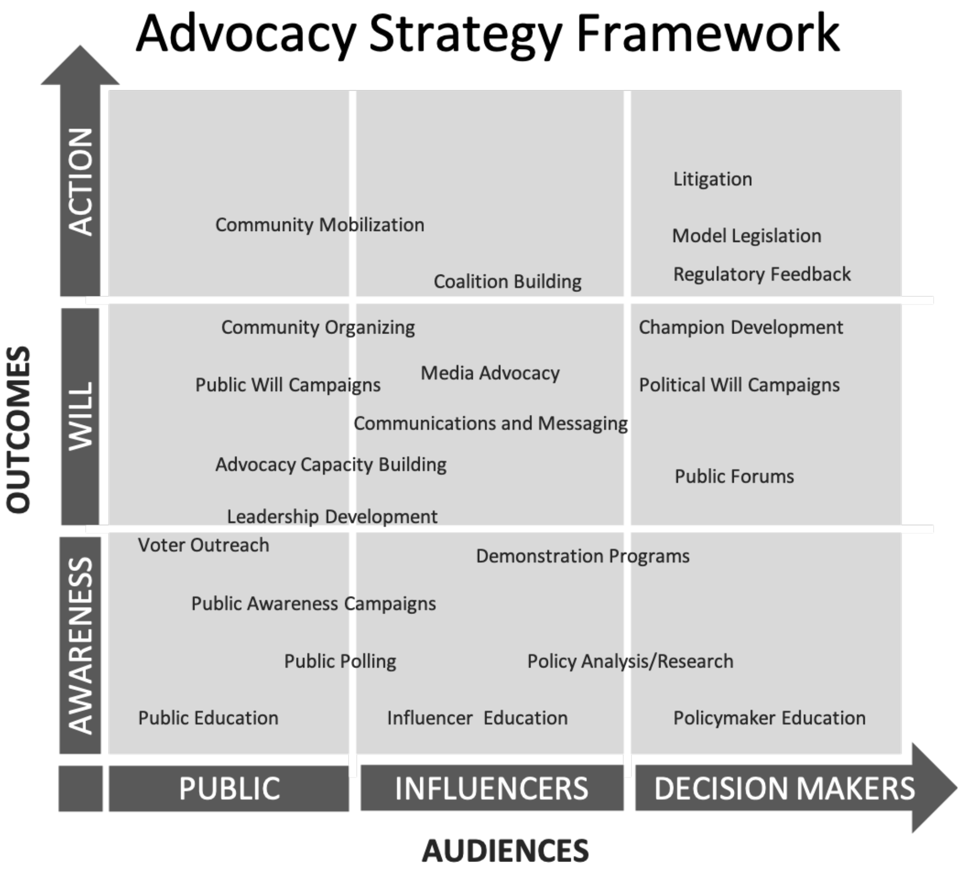


Figure 32: Advocacy Strategy Framework

Module 7: Online safety, vulnerability and intersectionality

Vulnerability can be defined as the likelihood or susceptibility of being harmed by unexpected circumstances, which occur within the social, economic, political contexts that interrelated with micro and macro environments.[20] Because of their young age, children are often considered as being more prone to vulnerabilities. Often vulnerabilities are multifaceted and intersect. Research shows that young people's situational vulnerabilities offline predicted high-risk online experiences.[21]

Aside from personal and individual or situational vulnerabilities, online safety risks occur within the societal and environmental contexts that children experience on a daily basis. From your PESTLE Analysis (Section 4.1 Stakeholder and Power Analysis), you might have identified issues in your country's context that might also be influencing children.

These can include poverty, climate change, conflict and terrorism, natural disasters, pandemics and economic crises, amongst others. Your organisation may already be working on some of these issues. The following are some ideas on how you can integrate key messages related to online safety in other advocacy efforts your organisation might be engaged in. You can research these issues further and identify any specific issues that might be relevant to your context to build your own message.

- Online safety risks, such as online violence against children or OCSEA, might be symptoms of other issues such as poverty and natural disasters.[22]

- Poverty can exclude children from accessing opportunities, which can make them vulnerable to several safeguarding issues, including exploitation. Sometimes exploitation can be presented as a way for children or family members to make money to address their situation.[23] Research also links poverty to child abuse.[24]

- Climate change exacerbates the risks of violence against children. Contexts experiencing population displacement, migration, and food scarcity show increases in child labour, child marriage, FGM, parental violence, wider gender-based violence, emotional harm and other risks.[25] The intersectionality of offline and online risks makes children more susceptible to online harms.

- Children are impacted the most by armed conflicts. Recent developments have seen an increase in cyberattacks and cyber-conflict, which can affect children in a range of ways. They can be targeted directly for recruitment into armed forces and armed groups. Children's personal data can be manipulated or stolen. Cyber tools can be used to spread misinformation and disinformation. Indirectly, children can be impacted through cyber-attacks on infrastructural sectors that are critical to child well-being, such as education and health.[26,27] Online, terrorist or violent extremist groups can also recruit children.[28]

- Disasters create child protection issues on multiple levels, including increased vulnerability to physical and sexual violence.[29]

- The Covid-19 pandemic provided clear evidence that children can become more susceptible to several risks, including online risks such as OCSEA when they are online.

- Not focusing on online risks and safety during times of economic crises can backfire. Education and awareness campaigns are an investment as the harms that result from being exposed to online risks can have a larger, longer-term social cost.

In Sweden, Barnfonden conducted study to explore the links between climate change, online safety, and violence against children by consulting researchers, non-government organizations (NGOs), and community-based organizations (CBOs), and activist groups. The research identified forced marriage, child labor and migration as issues where climate change and online safety intersect.

Moreover, climate activism requires bravery because it involves speaking out, often against authority. The research identified that young people who use social media in their activism efforts, exposed themselves to identification, abuse, vitriol and sometimes retribution because of speaking out.

barnfonden
Member of ChildFund Alliance

Climate change, violence against children and emerging online concerns

Summary of a segment of research from the paper, *Climate change and violence against children: Why care?*

Sounding the alarm: Concerns that the internet is being used to facilitate harm to climate-affected children.

Figure 33: Climate change, violence against children and emerging online concerns, published by Barnfonden.

Module 8 Case Study: ChildFund Ecuador Naveguemos Seguros

In Ecuador, internet safety is a topic that generates a lot of interest among parents and children. However, the State has not yet assumed a proactive role in the protection of children and adolescents, and the participation of young people in the formulation of public policies which impact them is insufficient. They are also absent in many decision-making spaces.

In Ecuador, digital violence affects thousands of girls and boys and, according to several studies carried out in the Americas, it increased significantly during the pandemic as technology use rose.

ChildFund Ecuador has limited financial resources to support and implement all the initiatives we could engage in, but nonetheless we consider our role as online safety advocates to be very important. We have now developed and implemented a detailed online safety advocacy program in Ecuador, and provide here further information which can be used by other members of the ChildFund network to develop similar initiatives.

> *"At ChildFund Ecuador, we consider that the protection of children and adolescents not only includes the physical but also the digital environments to which they are exposed. It is essential to articulate actions that help prevent risks in both the public and private spheres."*
> ***Maria Cristina Barrera, Director of ChildFund Ecuador***

ChildFund Ecuador's Naveguemos Seguros (Let's Navigate Safe) is an online safety initiative which focuses on both child protection and child participation. The Ecuadorian State's public policies include a responsibility to promote digital rights, including A Safe Internet for Children and Adolescents, the Digital Educational Agenda, and the Digital Agenda of Ecuador.

Within this framework, ChildFund has created alliances, with both public and private entities as well as the media, to encourage them to join the initiative and increase awareness and visibility of digital violence against children and adolescents.

Our political advocacy strategy aims to incorporate into regulations and public policy actions from different public institutions and social actors to promote the digital rights of young people and to prevent online violence, sexual violence in particular.

Naveguemos Seguros also offers digital education tools and education to parents, caregivers, and teachers, to promote digital rights and prevent digital violence against girls, boys, adolescents and young people within the framework of Ecuador's public policies on the safe use of the internet.

The actions within ChildFund Ecuador's strategy (Module 2) follow the principles of:

- digital education and formation of intergenerational networks,
- active participation,
- protection against exploitation, harassment and violence,
- right to privacy,
- articulation and cooperation,
- sensitization, and
- generation of information for advocacy.

The main objective (Section 2.3) for Naveguemos Seguros is to influence different levels of the State, society, and families to contribute to a framework for the protection of children and adolescents against violence in the digital world, particularly sexual violence, through the safe use of the Internet. More specifically, the initiative focuses on:

- the promotion of digital rights and the prevention of and attention to digital violence against children and adolescents, through advocacy and support to state entities;
- the training of parents, children and adolescents who participate in ChildFund's programs, developing skills and competencies to recognize the main risks associated with digital violence and mitigate them;
- the development of guides and innovative tools to understand and address the problem; and
- the implementation of communication campaigns to raise awareness among the population.

The main stakeholders (Module 4) are children and young people, parents and guardians, educators, communities, the technology sector, the government, non-governmental organizations and international non-governmental organizations, local partners, and the media.

Specifically, ChildFund Ecuador is aiming to reach over 4 million children and adolescents and 50% of their families, over 200,000 educational authorities, teachers and DECE officials and almost 16,000 educational institutions.

To achieve this, Child Fund Ecuador has established partnerships (Module 6) with several entities, including the Ministry of Education, the National Cybercrime Police, the National Council for Intergenerational Equality, the National Council for Gender Equality, Cotopaxi and Tungurahua Associations Corporation (CACTU), Federation of Community Organizations of Imbabura (FOCI), Ecuadorian Federation of the Northwest of Pichincha for Community Development (FENPIDEC), Federation of Organizations for Children and Adolescents of Pichincha (FONAP), Federation of Community Associations of Carchi (FEDACC).

More specifically, Naveguemos Seguros has been developed in line with the Model National Response[30] created by the WeProtect Global Alliance:

Society & Culture

1. Work with the Community: To engage the community (Section 6.5), ChildFund Ecuador developed guides and recreational tools aimed at parents and caregivers, children and adolescents, teachers, public, non-governmental and corporate officials on safe navigation, according to the framework of the competencies and responsibilities of each actor (Sections 4.3 and 6.6). These tools are promoted through workshops, fairs and on the ChildFund Ecuador website (Figure 34). During July 2021. There were over 27,000 unique visits to the page. ChildFund Ecuador also conducted a series of 7 webinars with the National Council for Intergenerational Equality and 18 public and private organizations to promote dialogue among key actors.

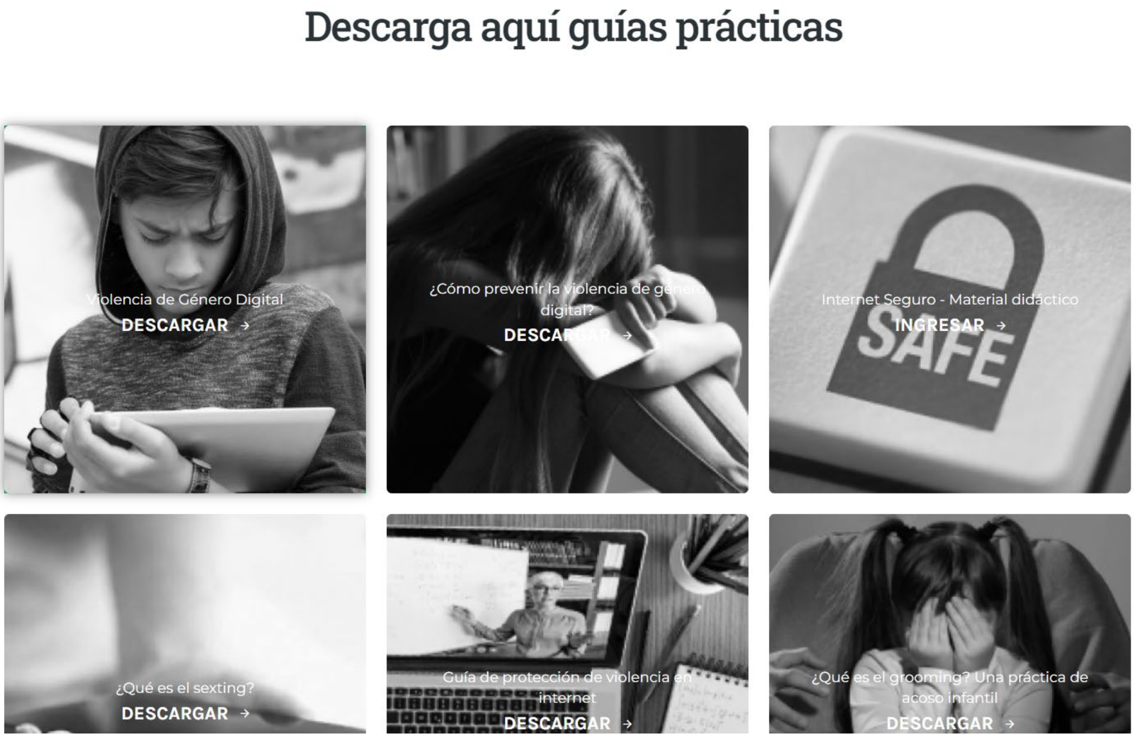

Descarga aquí guías prácticas
Violencia de Género Digital
DESCARGAR →
¿Cómo prevenir la violencia de género digital?
DESCARGAR →
Internet Seguro - Material didáctico
INGRESAR →
¿Qué es el sexting?
DESCARGAR →
Guía de protección de violencia en internet
DESCARGAR →
¿Qué es el grooming? Una práctica de acoso infantil
DESCARGAR →

Figure 34: Some of the Guides and Tools available on the ChildFund Ecuador Website

2. Safe and Protected Childhood Program: This was developed by ChildFund through its local partners in Carchi, Imbabura, Pichincha, Cotopaxi and Tungurahua. Together, they created content and tools with children and adolescents and their families, which allowed them to enhance the use of information communication technologies (ICTs) for education, communication, recreation and participation. At the same time, they learnt how to recognize the main risks associated with digital violence and mitigate them. The partners have reached 47,772 girls and boys with workshops and sessions on the safe and responsible use of ICTs and social networks for advocacy and social change, and 1,122 tablets with parental control applications were also delivered with 12,135 monthly recharges. This enabled girls, boys and adolescents to access the internet and continue with tele-education during the pandemic.

3. Digital campaign Ahora ya Sabes, #NaveguemosSeguros: The campaign (Section 6.1) aims to raise awareness about the threats and risks to which children and adolescents are exposed to online; increase the visibility of the problem; prevent risks; and use a positive approach to teach parents, adolescents, caregivers and teachers about online safety. During 2022, particularly in February and March, the campaign was promoted on social media (Figure 35) and traditional media (radio and TV) to raise awareness about safe surfing (February 2022) and to prevent and eradicate gender violence in the digital world (March 2022). In February 2022, the campaign reached 1,990,266 million people through traditional media boosting the #naveguemosseguros campaign. Two webinars were also held for Safer Internet month. With the #quetalsi Campaign in March 2022, a European Union initiative that seeks to raise awareness among citizens about the dangers that exist in digital spaces and promote safe internet use, 11,000,000 people were reached through traditional media.

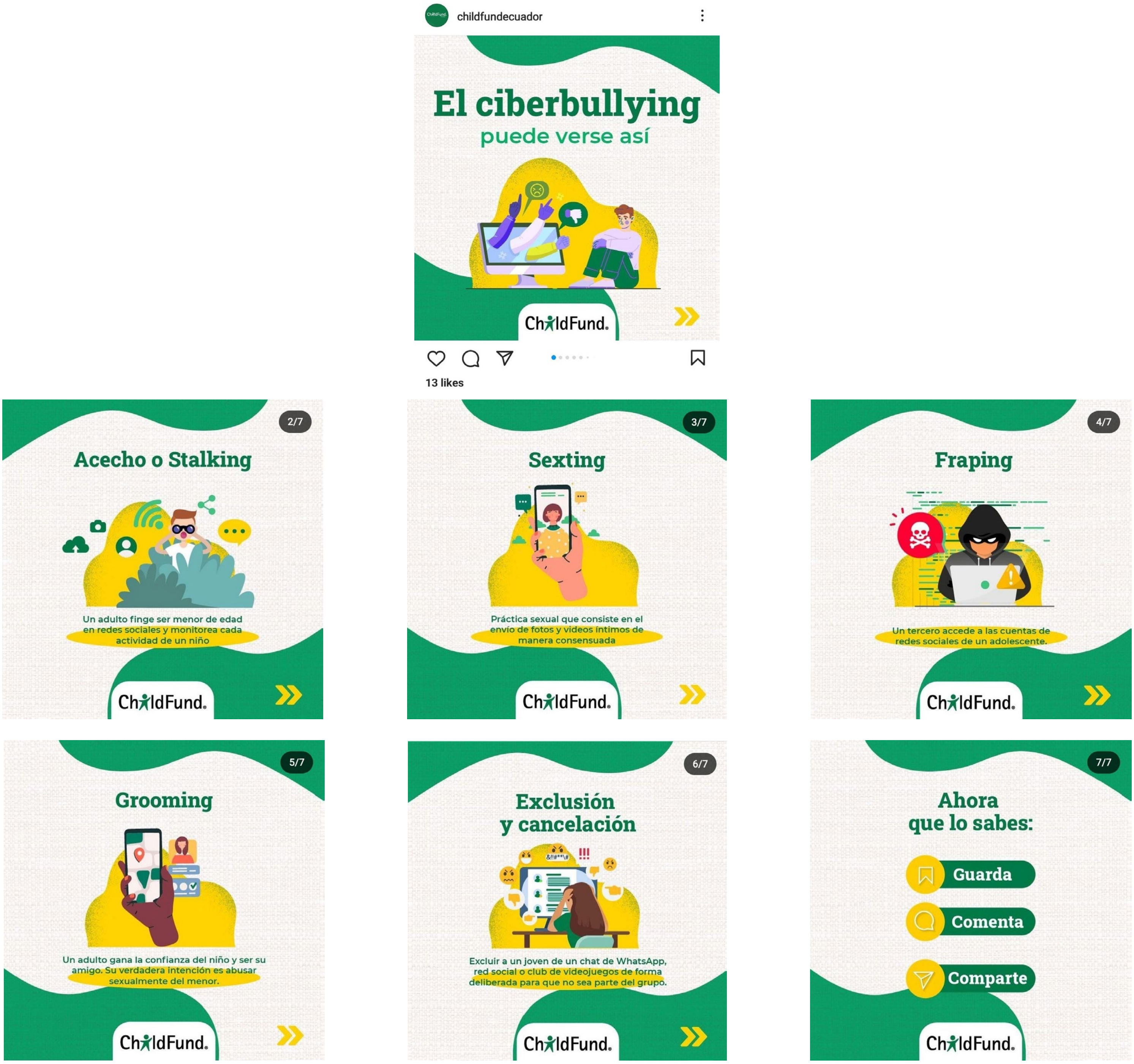

childfundecuador
El ciberbullying
puede verse así
ChildFund.
13 likes
2/7
Acecho o Stalking
Un adulto finge ser menor de edad en redes sociales y monitorea cada actividad de un niño
ChildFund.
3/7
Sexting
Práctica sexual que consiste en el envío de fotos y videos íntimos de manera consensuada
ChildFund.
4/7
Fraping
Un tercero accede a las cuentas de redes sociales de un adolescente.
ChildFund.
5/7
Grooming
Un adulto gana la confianza del niño y ser su amigo. Su verdadera intención es abusar sexualmente del menor.
ChildFund.
6/7
Exclusión y cancelación
Excluir a un joven de un chat de WhatsApp, red social o club de videojuegos de forma deliberada para que no sea parte del grupo.
ChildFund.
7/7
Ahora que lo sabes:
Guarda
Comenta
Comparte
ChildFund.

Figure 35: A ChildFund Ecuador Instagram campaign on cyberbullying

Research & insights

4. Generation of Information for Advocacy: ChildFund Ecuador is implementing the pilot of the OSEAC Pathway by ChildFund, and conducting a USI-OSEAC Survey to identify the risks faced by children and adolescents in the digital world (Section 3.3). The analysis of the results will be carried out in March 2023.

Policy & legislation

5. Regulatory axis: ChildFund Ecuador is seeking to position the importance of guaranteeing the digital rights of children and adolescents and create a legal framework that guarantees these rights. Together with 21 public and private institutions, we have contributed to the drafting of public policy (Section 5.2) for a safe internet for children and adolescents. This was sent to the National Assembly contributions on digital rights of children and adolescents for the proposed reform of the Comprehensive Organic Code of Children and Adolescents. We have also contributed to the National Assembly on online sex crimes against children and adolescents for the reform of the Comprehensive Organic Criminal Code. In this area, spaces for participation have been created for children to propose solutions to the problem of violence on the Internet.

6. Development of a Digital Culture: Through the alliances established (Section 6.4) with the Ministry of Telecommunications and Information Society, the Telecommunications Regulation and Control Agency, the Ministry of Education, the National Cybercrime Police, the National Council for Intergenerational Equality between other public actors, ChildFund promotes safe internet use and the implementation of mechanisms to protect children and adolescents from violence in the digital world.

In 2023, ChildFund Ecuador is contributing to the efforts of the Ministry of Education of Ecuador and supporting the prevention and awareness of the risks and violations of the rights of children and adolescents in online environments. It is also supporting the detection of risks and notification of suspected cases within the National Education System. Within the framework of the agreement with the Ministry of Education, the following activities are being carried out:

- Preparation of a guide, protocol and regulations against risks and violation of children and adolescents' rights in online environments.
- Support the detection of risks and reporting of suspected cases within the National Education System aligned with current protocols, the Organic Law of Intercultural Education (LOEI), and current legal regulations.
- Virtual pedagogical tools will also be developed and implemented: eg, Chatbot, Podcast, virtual routes of awareness and training.

The success of Naveguemos Seguros is due to its innovative techniques. It has incorporated various stakeholders and established important alliances, developed a policy, but also included information and materials targeting other stakeholders, namely children, and their parents, guardians and educators.

A key outcome of the program is the collaboration with the Ministry of Education. Through this collaboration the development of protocols is key. Such protocols are aimed at ensuring the sustainability within the institution itself, together with the quality of its outcomes. Furthermore, they also work for the continuity of the dissemination of the resources and to consolidate resources for online safety in the future budgets of the Ministry of Education. This alliance with the Ministry also allows the protocols to have a national and multi-year scope and potentially reach the entire educational system. In a second phase, ChildFund Ecuador will develop educational communication products to enhance the reach and familiarity with the protocols.

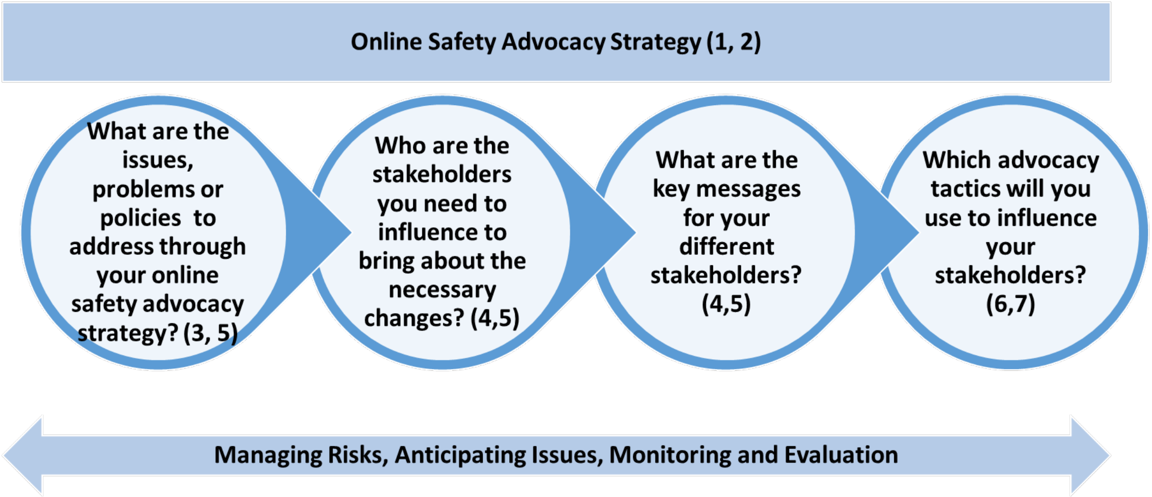
This project reflects the idea that alliances such as the one with the Ministry of Education are essential in order to scale impact for children. It also supports young people to become agents of change in relatively new field that impacts them directly. Naveguemos Seguros highlights the importance of developing communication materials that address the misinformation and lack of information that exists in Ecuador. Through a concerted effort targeting multiple levels and stakeholders, this information is disseminated widely to ensure the maximum reach. The solution is based on the evidence that information and its access is a fundamental tool to raise awareness on online safety issues. As demonstrated by UNICEF's (2015) results[31], violence against children has gained visibility on national agendas, with increased legislative activity, awareness and information campaigns, and other initiatives to improve data on children's experiences online.

Other outcomes of the Naveguemos Seguros project include:

- A political advocacy strategy to incorporate into regulations and public policy actions to promote the digital rights of children and adolescents and prevent online violence.
- Micro-learning pieces, guides and infographics that provide alerts to the risks that children and young adults face in the digital world. These are especially useful where young people do not have the support of adults. The contents of these guides and games collect key ideas and are then contextualized, allowing them to identify the risks (eg, grooming, sextortion or bullying), and develop critical thinking and skills to help them identify violent and dangerous content and know how to act and protect themselves.
- Gamified tools aimed at children and young people to raise awareness and develop practices for the safe use of the Internet. The Stairs and Slides game is adapted for a web environment that helps the development of computational thinking in girls and boys. The same game has a physical version that supports complementary actions of the Safe and Protected Childhood program model.
- The formation of alliances with public and private entities, as well as the media, has allowed us to generate a greater impact through awareness and visibility of digital violence against children and adolescents.

Conclusion

Figure 12 presents a visual summary of how to go about your online safety advocacy strategy. The numbers in brackets indicate which module to refer to in this toolkit to obtain further information about each aspect.


Online Safety Advocacy Strategy (1, 2)

What are the issues, problems or policies to address through your online safety advocacy strategy? (3, 5)

Who are the stakeholders you need to influence to bring about the necessary changes? (4,5)

What are the key messages for your different stakeholders? (4,5)

Which advocacy tactics will you use to influence your stakeholders? (6,7)

Managing Risks, Anticipating Issues, Monitoring and Evaluation

Figure 35: Online Safety Advocacy Strategy summary

Remember, you do not need to do everything that is presented in this toolkit in one go! Strategize carefully based on the resources you have available and build experiences as you go along. It is not expected that your advocacy strategy will transform the field of online safety in your country overnight. However, there are measured steps you can take to achieve the necessary changes over time.

Useful links and other resources

Five Rights Foundation: Online Safety Toolkit: https://childonlinesafetytoolkit.org/

AT&T + APA: Screen Ready: https://screenready.att.com/digital-parenting/

Council of Europe: Lanzarote Convention: https://www.coe.int/en/web/children/lanzarote-convention

Digital Trust & Safety Partnership: Best Practices Framework for the Technology Industry: https://dtspartnership.org/best-practices/

ECPAT: Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse: https://ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines-396922-EN-1.pdf

ESRB: Family Gaming Guide: https://www.esrb.org/tools-for-parents/family-gaming-guide/
International Telecommunication Union - Child Online Protection (COP) Guidelines: https://www.itu-cop-guidelines.com/

WeProtect Global Alliance: Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response: https://www.weprotect.org/model-national-response/

WHO: What works to prevent violence against children online?
https://www.who.int/publications/i/item/9789240062061

Appendix A: Glossary of key terms and definitions

A

Artificial Intelligence (AI) classification or AI moderation: Automated or partly-automated moderation systems that identify harmful content by following rules and interpreting many different examples of content, which is and is not harmful.[32]

B

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.[33] A glossary focused on cyberbullying is available here.

C

Capping: Offenders capturing footage of livestreamed child sexual abuse and exploitation. Capping may also include offenders capturing innocuous imagery of children and using it for sexual purposes (this imagery would then constitute sexualized images of children).[32]

Child displaying harmful sexual behavior: A child or young person under the age of 18 years old exhibiting behaviors that are developmentally inappropriate, may be harmful towards themselves or others and/or abusive towards another child, young person or adult.[32]

Child protection systems: Certain formal and informal structures, functions and capacities that have been assembled to prevent and respond to violence, abuse, neglect and exploitation of children. A child protection system is generally agreed to be comprised of 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. Most important are the relationships and interactions between and among these components and these actors within the system. It is the outcomes of these interactions that comprise the system (UNICEF/UNHCR/Save the Children/World Vision, 2013, p. 3).[34]

Child 'self-generated' sexual material: Content of a sexual nature, including nude or partially nude images and video, that has been produced by children of themselves. There are scenarios in which harm is caused, primarily:
- When a child or adolescent is coerced into producing 'self-generated' sexual material
- When voluntarily 'self-generated' sexual material is shared against an adolescent's wishes.[32]

Child sexual abuse: The harm caused to children [anyone under 18] by forcing or coercing them to engage in sexual activity, whether they are aware of what is happening or not. It is defined as the involvement of a child in sexual activity that he or she does not fully comprehend, is unable to give informed consent to, or for which the child is not developmentally prepared, or else that violates the laws or social taboos of society.

Children can be sexually abused by both adults and other children who are – by virtue of their age or stage of development – in a position of responsibility, trust or power over the victim. The sexual abuse of children requires no element of exchange and can occur for the mere purpose of the sexual gratification of the person committing the act. Such abuse can be committed without explicit force, with other elements, such as authority, power or manipulation being determining factors.[32,35]

Child sexual abuse live streaming: Where adults pay a fee in order to direct and view a live video of children performing sexual acts in front of a webcam.[36] It is transmitted in real-time over the internet.

Child sexual abuse material (CSAM): Sometimes referred to as 'child pornography' as well as digitally-produced CSAM, 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 per cent increase over figures reported in 2018. Many more remain undetected.[37]

Child sexual exploitation: A form of child sexual abuse that involves any actual or attempted abuse of a position of vulnerability, differential power or trust. This includes, but is not limited to, profiting monetarily, socially or politically from the sexual exploitation of another. Individuals or groups of offenders can perpetrate this. What distinguishes child sexual exploitation from child sexual abuse in the underlying notion of exchange present in exploitation. There is significant overlap between the two concepts, because exploitation is often a feature of abuse, and vice versa.[32]

Chat roulette: A network of users where strangers can interact with other strangers over text-chat, webcam and microphone, choosing to 'take part' or 'observe'. This is not suitable for children as many users post sexual images and there could be a risk of grooming.[38]

Child trafficking: The recruitment, transportation, transfer, harboring or receipt of a child for the purpose of exploitation.[32]

Circumventor sites: Parallel websites that allow children to get around filtering software and access sites that have been blocked.[39]

Clickjacking: A malicious technique of tricking a user into clicking on something different from what the user perceives, thus potentially revealing confidential information or allowing others to take control of their computer while clicking on seemingly innocuous objects, including web pages.[40]

Closed systems: A limited network of sites that are rated and categorized by maturity level and quality. Within a closed system, children cannot go beyond the network whitelist of approved websites, also referred to as a "walled garden."[39]

Commercial sexual exploitation of children (CSEC): A form of sexual exploitation where the focus is specifically on monetary benefit, often relating to organized criminality where the primary driver is economic gain.[41]

Computer-generated imagery (CGI): In the context of child sexual abuse and exploitation, this refers to wholly or partly artificially or digitally created sexualized images of children.[32]

Conduct risks: Potential harm based on the behaviour or conduct of the user or their peers, e.g. deliberately using online platforms to threaten or harass other users, including cyberbullying, "sexting" and hateful comments, sometimes also unintentionally by disclosure of private information of other users.[4]

Contact risks: Potential harm created by the opportunity for users to contact each other using online services, e.g. enabling strangers or people hiding their identity to contact children.[4]**Error! Bookmark not defined.**

Content risks: Potential harm to users based on the nature of online content, including age-inappropriate (e.g. pornography), unreliable (e.g. misinformation or disinformation) or certain other categories of content (e.g. promoting risky behaviour or methods of self-harm or suicide).[4]

Contract risks: Potential harm wherein a user is exposed to inappropriate commercial contractual relationships or pressures, e.g. compulsive use, gambling, targeted advertising, hidden costs, unfair terms and conditions, and loss of control of personal data.[4]

Crosscutting risks: Some risks relate to most or all of the four categories and can have multiple manifestations across the different dimensions (aggressive, sexual, values). These include online risks relating to privacy, physical or mental health, inequalities or discrimination.[4]

Cybercrime: Any internet-related illegal activity.[39]

Cyber defamation: Using words or images or signals online to lower the reputation or prestige of the target.[42]

Cyber-enticement: An individual communicating with someone believed to be a child via the internet with the intent to commit a sexual offense or abduction.[43]

Cyber extremism: Ideological indoctrination and recruitment, threats of extreme violence using any online or digital platform, beyond the norms of existing common social way of life.[4242]

Cyber flashing: When someone sends an inappropriate, often sexually explicit, photo to someone else. This might be through standard text messaging, dating sites or social media but can also happen through Airdrop on Apple devices or other means that use Bluetooth. These images are sent without consent of the recipient. In some cases, the recipient may see a preview of the image being sent to them through Bluetooth. This means that even if they refuse the image, they will have already seen part of it. As such, this could be especially harmful for young people. When one child or young person cyber flashes another child or young person, this is a form of child-on-child (or peer-on-peer) abuse.[38]

Cyber harassment: Messaging abusive or other objectionable content to the target child or creating fake profiles in social media with the intention of targeting him or her.[42]

Cyber intimidation: Communicating direct or implied threats through emails or messages in social media to inspire fear in the target child.[42]

Cybersecurity: Any technique, software, etc., used to protect computers and prevent online crime.[39]

Cyber stalking: Following someone on Internet/mobile for causing inconvenience, or harassment/extortion, or for other illegal motives.[42] Methods individuals use to track, lure, or harass another person online.[39]

D

Dark web: The layer of information and pages that you can only get access to through so-called 'overlay networks' (such as Virtual Private Networks (VPN) and peer-to-peer (P2P) file sharing networks), that obscure public access. Users need special software to access the dark web because a lot of it is encrypted, and most dark web pages are hosted anonymously.[32]

Deep fake: A form of CGI that uses artificial intelligence to replace one person's likeness with another in photos or recorded video.[32]

Deep web: The portion of the web whose contents are not indexed by standard web search engines, and includes many common uses such as webmail, online banking, and subscription services. Content can be located and accessed by a direct link or IP address and may require a password or other security access beyond the public webpage.[44]

Digital citizenship: The ability to navigate digital environments in a way that is safe and responsible and to actively and respectfully engage in these spaces.[45]

Digital footprint: A digital footprint – sometimes called a digital shadow or an electronic footprint – refers to the trail of data left when using the internet. It includes websites visited, emails sent, and information submitted online. A digital footprint can be used to track a person's online activities and devices. Internet users create their digital footprint either actively or passively.[46]

Digital literacy: The ability to use information and communication technologies to find, evaluate, create, and communicate information, requiring both cognitive and technical skills.[47]

Doxxing: When someone on the internet (the doxxer) posts personal information about someone else (the victim) for the world to see. This information is sensitive, meaning it can be used to figure out who someone really is, where they live and how to contact them.[32]

E

Encryption: The process of encoding information into an alternative form that can only be decrypted by authorized individuals who possess the decryption key.[32]

End-to-end encryption: A form of encryption wherein the content of each message is visible only to the sender and recipient. Unscrambling the message requires a private decryption key exchanged between correspondents, so that while the message may be intercepted, it cannot be viewed or monitored by the service provider, law enforcement or any other third party.[32]

Exposure: Public display, posting or forwarding of personal and private communication, images or video of the target child.[42]

F

'First generation' child sexual abuse material: Child sexual abuse material that has not previously been detected and classified by law enforcement and / or moderators.[32]

Flame: An offensive or aggressive message sent to a specific person over the internet.[38]

G

Gamification of abuse: The application of game-like elements (e.g. point scoring, competition with others, rules of play) to encourage participation in abuse and exploitation.[32]

Grooming children online for the purpose of sexual exploitation and abuse: An individual builds a relationship, trust and emotional connection with a child or young person to manipulate, exploit and abuse them (facilitated, partly or entirely, by the internet or other wireless communications). There is not always an intent to meet in person. Also known by the term 'online enticement'.[32]

Grooming: Actions deliberately undertaken with the aim of befriending and establishing an emotional connection with a child, in order to lower the child's inhibitions in preparation for sexual activity with the child.[48]

H

Habit formation and online enticement to illegal behaviors: Access to alcohol, cheating, plagiarism, gambling, drug trafficking, sexting and self-exposure.[42]

Hate speech: Hate speech includes statements intended to demean and brutalise another and the use of cruel and derogatory language on the basis of real or alleged membership in a social group. This includes racism and xenophobia.[49]

Hashing: A process whereby a binary hash is created by a mathematical algorithm that transforms data of any size into much shorter fixed-length data. This shorter sequence represents the original data and becomes this file's unique signature, or its hash value – often called its digital fingerprint.[32]

Hash matching: A process of using databases of hashed child sexual abuse material to detect when the material is re-shared, by matching its hash value against those of already known files.[32]

Hidden services: Websites that are hosted within a proxy network (such as Tor), so their location cannot be traced.[32]

I

ICCAM: ICCAM enables the secure exchange of illegal material portraying child sexual abuse between hotlines located in different jurisdictions, with the aim of quick removal from the internet. ICCAM also provides a service to hotlines worldwide to classify images and videos according to international standards (INTERPOL's criteria) as well as national laws – all in one system.[50]

Image-based abuse: Sharing or threatening to share intimate images or videos of a person without their consent. This can include photos, screenshots and photoshopped or fake content. Alternative terms for image-based abuse include 'non-consensual sharing of intimate images', 'revenge porn' or 'intimate image abuse'. Sextortion is a type of image-based abuse. This type of abuse also includes digitally altering a photo or video (for example, by photoshopping) or depicting a person without religious or cultural attire, which they would usually wear in public. Even threatening to share intimate images in this way is image-based abuse. It is a criminal offence under state and territory laws.[51]

Industry code: A code regulating the conduct of participants in an industry towards other participants in the industry or towards consumers in the industry.[52]

Instant message/messaging (IM): Private, real-time text conversation between two users.[39]

International Child Sexual Exploitation (ICSE) Database: Managed by Interpol, the International Child Sexual Exploitation (ICSE) image and video database is an intelligence and investigative tool used by specialized investigators to share data on cases of child sexual abuse around the world.[53]

J

Jailbait: Someone who is under the age of consent but who dresses, acts and appears as if they are over the age of consent and who does nothing to correct that impression.[38]

K

Known child sexual abuse material: Child sexual abuse material that has been previously detected and classified by law enforcement and/or moderators.[32]

L

Livestreaming child sexual exploitation and abuse: Transmitting child sexual abuse and exploitation in real-time over the internet. This occurs on online chat rooms, social media platforms, and communication apps with video chat features. Viewers of livestreaming child sexual abuse can be passive (pay to watch) or active by communicating with the child, the sexual abuser and/or facilitator of the child sexual abuse, and requesting specific physical acts. Another form of livestreaming can involve coercing a child to produce and transmit sexual material in real-time.[54]

M

Metadata: Data that describes other data. Examples of metadata would include the time and duration of a phone call (as opposed to the content of the communication itself).[32]

Monitoring software: Software products that allow parents to monitor or track the websites or e-mail messages that a child visits or reads.[39]

N

Non-graphic CSAM: Non-graphic child sexual violations including audio, text, and artistic renderings. These instances of abuse, which have flown under the radar in some instances, exist on UGC platforms in much larger quantities than graphic CSAM. Because these violations are complex and nuanced, they are therefore much harder to detect.[55]

Non-photographic child sexual abuse material: This includes computer-generated images cartoons, or drawings, which graphically depict children in a sexually abusive way.[32]

O

Online Child Sexual Exploitation and Abuse (OCSEA): Child sexual exploitation and abuse that is partly or entirely facilitated by technology, i.e. the internet or other wireless communications."[32]

Online predator: A person who sexually exploits one or more children over the Internet (or attempts to).[56]

Online sexual exploitation of children: The use of the Internet as a means to exploit children sexually. Indeed, the terms 'ICT-facilitated' and 'cyber-enabled' child sexual exploitation are sometimes used as alternatives to define these practices. The reference to "online child sexual exploitation" includes all acts of a sexually exploitative nature carried out against a child that have, at some stage, a connection to the online environment. It includes any use of ICT that results in sexual exploitation or causes a child to be sexually exploited or that results in or causes images or other material documenting such sexual exploitation to be produced, bought, sold, possessed, distributed, or transmitted.[57]

Online sexual harassment: Unwelcome sexual advances, request or demand for 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 (i.e., purpose) but also to conduct of a sexual nature that a person experiences as offensive or intimidating.[42]

P

Parental controls: specific features or software that allow parents to manage the online activities of children.[39]

Privacy by Design: Data protection through technology design. Behind this is the thought that data protection in data processing procedures is best adhered to when it is already integrated in the technology when created.[58]

Producing child sexual and abuse material: Creating child sexual abuse material by in-person photography/video/audio recording; creating textual content or non-photographic (for example, computer-generated) visual material; or manipulating existing child sexual abuse material to create new unique imagery.[32]

Protective factors: Factors at the individual, relationship, community, and societal level that may reduce the risk of a child being a victim of sexual abuse and exploitation.[32]

R

Real-time: "Live" time; the actual time during which something takes place.[39]

Revenge Pornography: The distribution of sexually explicit images or videos of individuals without their consent.

Re-victimization: When a victim faces any sexual abuse or assault subsequent to a first abuse or Assault. This includes the further distribution and viewing of imagery on the internet: a single image of a victim can be shared hundreds or thousands of times. Re-victimization may be caused by the same or a different offender to the initial victimization.[32]

Risk factors: Factors at the individual, relationship, community, and societal level that may make a child more likely to experience sexual abuse and exploitation.[32]

S

Safety-by-design: The embedding of the rights and safety of users into the design and functionality of online products and services from the outset.[32]

Safety technology (safety tech): Solutions to facilitate safer online experiences, and to protect users from harmful content, contact or conduct.[32]

Searching for and/or viewing child sexual abuse material: Seeking child sexual abuse material on the internet and viewing or attempting to view it.[32]

Self-generated CSAM: Sexually explicit content created by and featuring children below the age of eighteen. These images can be taken and shared intentionally by minors, but are in many cases a result of online grooming or sextortion.[59]

Sexting: The the 'self-production of sexual images', or as 'the creating, sharing and forwarding of sexually suggestive nude or nearly nude images through mobile phones and/or the internet'. It is a frequent practice among young persons and often a consensual activity between peers. There are also many forms of 'unwanted sexting'. This refers to the non-consensual aspects of the activity, such as sharing or receiving unwanted sexually explicit photos or messages.[60]

Sextortion: The blackmailing of a person with the help of (self-generated) images of that person in order to extort sexual favors, money, or other benefits from her/him under the threat of sharing the material beyond the consent of the depicted person (e.g. posting images on social media). When carried out against children, sexual extortion involves a process whereby children or young people are 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.[60]

Sexualized material of children: Material that does not represent the sexual abuse of a child, but which is used for sexual purposes. An example might be a video of children doing gymnastics, which is inappropriately viewed for sexual gratification. Sexualization is not always an objective criterion, and the crucial element in judging such a situation is the intent of a person to sexualize a child in an image or to make use of an image for sexual purposes.[32]

Sexual exploitation: This Is distinguished from other forms of child sexual abuse by the underlying notion of exchange present in exploitation.[61]

Sexual exploitation of children in travel and tourism (SECTT): Acts of sexual exploitation of children, which are embedded within the context of travel, tourism or both.[62]

Sharing and/or storing child sexual abuse material: Downloading, storing, hosting, uploading and/or sharing child sexual abuse material.[32]

Social exclusion: Using online platforms to message the target child that he or she is not included with the peer group and its social activities.[42]

Social media: The collective of online communications channels dedicated to community-based input, interaction, content-sharing and collaboration. Websites and applications dedicated to forums, microblogging, social networking, social bookmarking, social curation, and wikis are among the different types of social media.[42]

Solicitation of Children for Sexual Purposes: The solicitation of children for sexual purposes is often referred to as "grooming" or "online grooming". It can be described as a practice by means of which an adult "befriends" a child (often online, but offline grooming also exists and should not be neglected) with the intention of sexually abusing her/him.[63]

Surface Web: The portion of the web readily available to the public and searchable with standard web search engines.[32]

T

Tor: An open-source privacy network that permits users to browse the web anonymously. The system uses a series of layered nodes to hide web address, online data, and browsing history.[32]

Tradecraft: An ever-evolving host of cloaking techniques and evasion strategies offenders use to avoid individual detection, and their techniques and strategies for identifying and engaging children.[32]

V

Victim blaming: When the victim of a crime is seen as responsible for the harm they have experienced. For example, someone who has experienced image-based abuse may have consensually shared their intimate images with people in the first place. However, it is not their fault if someone later shares or threatens to share their image without consent.[38]

Videocam (webcam): Video cameras that are either attached or built into a computer so that a video image can be sent to another while communicating online.[39]

Virtual Private Network (VPN): An arrangement that creates an encrypted connection over the Internet from a device to a network, known as a tunnel.[32]

Virtualizing & emulation: Virtual machines allow users to run an operating system that behaves like a full, separate computer in an app window on their desktop. Some emulators can create a virtual smartphone interface on a computer. This allows the user to install and use apps on their computer that would otherwise not be available. Emulators are often used in conjunction with 'capping' tools, as they can prevent a 'screenshot' notification from being sent to the victim, and the offender can use 'capping' software installed on their computer to capture clearer images.[32]

Other Glossaries

https://childonlinesafetytoolkit.org/wp-content/uploads/2022/05/5Rights-Child-Online-Safety-Toolkit-English.pdf
https://cyberbullying.org/social-media-cyberbullying-online-safety-glossary.pdf
https://defendingdigital.com/glossary/
https://ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines-396922-EN-1.pdf
https://inhope.org/EN/articles/what-is
https://internetsafety101.org/glossaryofterms
https://www.interpol.int/en/Crimes/Crimes-against-children/Appropriate-terminology
https://www.e2bn.org/cms/e-safety/glossary-of-e-safety-terms
https://www.esafety.gov.au/about-us/glossary
https://www.internetmatters.org/resources/glossary/

Reference list

[1] www.learning.com/blog/online-safety-definition-basics/

[2] https://swgfl.org.uk/online-safety/what-is-online-safety/

[3] Staksrud, E., Livingstone, S., Haddon, L. & Ólafsson, K. (2009). What do we know about children's use of online technologies: A report on data availability and research gaps in Europe (2nd edn). EU Kids Online. http://eprints.lse.ac.uk/24367/

[4] Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. https://doi.org/10.21241/ssoar.71817

[5] Farrugia, L. (2020). Children and new media: a psychosocial approach to understanding how preadolescents make sense of online risks. (Unpublished PhD Dissertation). University of Malta, Malta. www.um.edu.mt/library/oar/handle/123456789/81313

[6] Stachowiak, S., Gienapp, A., & Reisman, J. (2007). A guide to measuring advocacy and policy. Anne Casey Foundation www.aecf.org/resources/a-guide-to-measuring-advocacy-and-policy

[7] Coffman, J., & Beer, T. (2015). The advocacy strategy framework. *Center for evaluation innovation.*

[8] Office of the United Nations High Commissioner for Human Rights. (1989). Convention on the rights of the child. (General Assembly resolution 44/25 of 20 November 1989). Geneva: United Nations. http://www.unicef.org/crc

[9] https://www.unicef.org.uk/what-we-do/un-convention-child-rights/

[10] https://digitallibrary.un.org/record/3906061?ln=en#record-files-collapse-header

[11] APSP (2017) Advocacy Tool Kit 'Be The Change You Want to See'

[12] Doran, G.T. (1981) There's a S.M.A.R.T. way to write management's goals and objectives. Management Review (AMA FORUM) 70 (11): 35–36.

[13] www.phoenixzonesinitiative.org/effective-advocacy-power-dynamics/

[14] www.powercube.net/wp-content/uploads/2011/04/powerpack-web-version-2011.pdf

[15] https://millneckinternational.org/resources/developing-advocacy-plan

[16] https://resourcecentre.savethechildren.net/document/education-we-want-advocacy-toolkit/

[17] https://ctb.ku.edu/en/table-of-contents/advocacy/direct-action

[18] https://ctb.ku.edu/en/table-of-contents/participation/promoting-interest

[19] https://ctb.ku.edu/en/table-of-contents/participation/promoting-interest/press-conference/main

[20] Dirks, J. M., & McIntyre, D. (2022). Societal Intersections and COVID-19 Effects on Young Children Vulnerability: A Transdisciplinary Approach to Holistic Integration. In Provision of Psychosocial Support and Education of Vulnerable Children (pp. 228-262). IGI Global.

[21] El Asam, A., & Katz, A. (2018). Vulnerable young people and their experience of online risks. *Human–Computer Interaction*, *33*(4), 281-304.

[22] Cerna-Turoff, I., Fischer, HT., Mansourian, H. et al. The pathways between natural disasters and violence against children: a systematic review. *BMC Public Health 21*, 1249 (2021). https://doi.org/10.1186/s12889-021-11252-3

[23] https://safeguarding.network/content/safeguarding-resources/impact-of-poverty/

[24] Bywaters, P., Skinner, G., Cooper, A., Kennedy, E., & Malik, A. (2022). The relationship between poverty and child abuse and neglect: new evidence. *London: Nuffield Foundation*.

[25] www.end-violence.org/articles/how-climate-crisis-driving-violence-against-children-and-what-we-can-do-about-it

[26] www.unicef.org/globalinsight/media/2856/file/UNICEF-Global-Insight-Rapid-Analysis-Protecting-Children-in-Cyberconflicts-2022.pdf

[27] www.unicef.org/blog/conflict-changes-so-do-dangers-children

[28] www.unodc.org/documents/justice-and-prison-reform/Child-Victims/Handbook_on_Children_Recruited_and_Exploited_by_Terrorist_and_Violent_Extremist_Groups_the_Role_of_the_Justice_System.E.pdf

[29] https://resourcecentre.savethechildren.net/pdf/what_is_child_protection.pdf/

[30] www.weprotect.org/model-national-response/

[31] www.unicef.org/lac/media/34481/file/Violence-against-children-full-report.pdf

[32] www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2021.pdf

[33] www.who.int/news-room/fact-sheets/detail/violence-against-children

[34] www.endvawnow.org/en/articles/1727-child-protection-systems.html

[35] https://inhope.org/EN/articles/what-is-child-sexual-abuse

[36] www.ohchr.org/en/stories/2016/03/new-digital-technologies-produce-unprecedented-levels-child-abuse-material-online

[37] https://ecpat.org/wp-content/uploads/2021/05/TOWARDS-A-GLOBAL-INDICATOR-ON-UNIDENTIFIED-VICTIMS-IN-CHILD-SEXUAL-EXPLOITATION-MATERIAL-Summary-Report.pdf

[38] www.internetmatters.org/resources/glossary/

[39] https://internetsafety101.org/glossaryofterms

[40] https://en.wikipedia.org/wiki/Clickjacking

[41] https://defendingdigital.com/glossary/

[42] www.icmec.org/wp-content/uploads/2016/09/UNICEF-Child-Protection-Online-India-pub_doc115-1.pdf

[43] www.missingkids.org/theissues/onlineenticement

[44] www.cisoplatform.com/profiles/blogs/surface-web-deep-web-and-dark-web-are-they-different

[45] https://mediasmarts.ca/digital-media-literacy/general-information/digital-media-literacy-fundamentals/what-digital-citizenship

[46] www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint

[47] https://literacy.ala.org/digital-literacy/

[48] https://inhope.org/EN/articles/grooming

[49] https://inhope.org/EN/articles/what-is-hate-speech

[50] https://inhope.org/EN/articles/iccam-what-is-it-and-why-is-it-important

[51] www.esafety.gov.au/about-us/glossary

[52] www.lawinsider.com/dictionary/industry-code

[53] https://inhope.org/EN/articles/what-is-the-international-child-sexual-exploitation-icse-database

[54] www.unicef.org/media/113731/file/Ending%20Online%20Sexual%20Exploitation%20and%20Abuse.pdf

[55] www.activefence.com/blog/non-graphic-csam-blindspot/

[56] https://defendingdigital.com/glossary/

[57] https://ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines-396922-EN-1.pdf

[58] https://gdpr-info.eu/issues/privacy-by-design/

[59] https://inhope.org/EN/articles/what-is-self-generated-csam

[60] https://ecpat.org/wp-content/uploads/2021/05/SECO-Booklet_ebook-1.pdf
[61] https://plan-international.org/uploads/2021/12/child_protection_and_resilience_final.pdf
[62] https://inhope.org/EN/articles/what-is-the-sexual-exploitation-of-children-in-travel-and-tourism
[63] www.infogreen.lu/Digitalisation-is-changing-the-world-Part-two.html

ChildFund®
Alliance

Every child deserves to live a life free from violence.

childfundalliance.org