ITUPublications

International Telecommunication Union
Development Sector

PoP: Protection through Online Participation

PoP guiding principles to facilitate children's access to protection and support through digital means

OFFICE OF THE SPECIAL REPRESENTATIVE OF THE SECRETARY-GENERAL ON
VIOLENCE AGAINST CHILDREN

Required citation:

ITU and the Office of the Special Representative of the Secretary General on Violence against Children, 2025. PoP: Protection through online Participation. Guiding principles to facilitate children's access to protection and support through digital means.

ISBN

978-92-61-41731-4 (PDF version)
978-92-61-41741-3 (Electronic Publication version)

Disclaimer

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the International Telecommunication Union (ITU) or of the ITU secretariat concerning the legal status of any country, territory, city, or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned. Errors and omissions excepted; the names of proprietary products are distinguished by initial capital letters.

All reasonable precautions have been taken by ITU to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader.

The opinions, findings and conclusions expressed in this publication do not necessarily reflect the views of ITU or its membership.

PoP: Protection through Online Participation

PoP guiding principles to facilitate children's access to protection and support through digital means

Ways forward for policy-makers, digital platforms, civil society organizations, child helplines and similar services

Acknowledgements

The PoP *guiding principles to facilitate children's access to protection and support through digital means* have been developed by the International Telecommunication Union (ITU) thanks to the partnership with the Global Cybersecurity Forum (GCF), and the Office of the Special Representative of the Secretary-General on Violence against Children (SRSG-VAC), together with a working group of contributing authors from leading institutions active in the areas of child rights, online safety, and digital policy.

The process was jointly led by Fanny-Carlotta Rotino (ITU) and Luisa Sotomayor (SRSG-VAC) and informed by extensive consultation and collaboration across sectors, including international organizations, civil society, academia, industry, and child protection practitioners.

The development of these PoP guiding principles would not have been possible without the time, expertise, and dedication of all contributing authors and reviewers. The drafting process benefited from valuable inputs received from a broad range of stakeholders who share a common commitment to advancing children's rights and ensuring safe, accessible, and empowering digital environments.

ITU and the Office of the Special Representative of the Secretary-General on Violence against Children are grateful to the following partners, who have contributed their valuable time and insights (listed in alphabetical order of organisation):

- John Zoltner (AIChildSafety.org)
- Michael Rich (Boston Children's Hospital – Digital Wellness Lab)
- Helen Mason, Anastasia Shuster (Child Helpline International)
- Awo Aidam Amenyah (Child Online Africa)
- Sonia Livingstone (Digital Futures for Children, Global Kids Online)
- Patricia Noel, Mauro Sanna (Discord)
- Francesco Cecon (ECPAT International)
- Hoda Alkhzaimi (EMARATSEC, Emirates Digital Association for Women, New York University Abu Dhabi)
- Fabiola Bas Palomares, Mieke Schuurman (Eurochild)
- Vasiliki Charisi (Harvard University – Berkman Klein Centre for Internet and Society)
- Manoel Fernando Alonso Gadi, Cristina Fernandez Tesoro (IE University)
- Fanny Rotino (ITU)
- Luc Delany, Kay Vasey (k-ID)
- Karen Scott (Lego)
- Maria-Cristina Capelo, Deepali Liberhan (Meta)
- Liz Thomas (Microsoft)
- Jennifer Kaberi (Mtoto News)
- Manus Debarra, Pablo Espiniella, Luisa Sotomayor (Office of the Special Representative of the Secretary-General on Violence against Children)
- Cliff Manning (Parent Zone)
- Henry Adams (Resolver)

- Tami Bhaumik, Laura Higgins (Roblox)
- Marija Manojlovic, Natalie Shoup, Serena Tommasino (Safe Online)
- Rebecca Smith (Save the Children)
- Jacqueline Beauchere, Viraj Doshi (Snapchat)
- David Wright (SWGfL, UK Safe Internet Centre)
- Jim Fruchterman, Nick Hurlburt (Tech Matters)
- Laura Rubbo (The Walt Disney Company)
- Elisha Ferguson, Christine Morrison, Elliot Taylor (Throughline Care)
- Matt Soeth (TIGG)
- Dan Mills, Valiant Richey (TikTok)
- Afrooz Kaviani-Johnson (UNICEF)
- Ha Ryong Jung, Alexandra Souza Martins (UNODC)
- Hilary Bakrie, Shihui Liu (UN Youth Office)
- Delali Mortty (WeProtect Global Alliance)
- Amanda Third (Western Sydney University – Young & Resilient Research Centre)

This publication forms part of ITU's Global Child Online Protection (COP) Initiative, under the Global Programme "Creating a Safe and Prosperous Cyberspace for Children", implemented in partnership with the Global Cybersecurity Forum (GCF). This programme aligns with the wider Child Protection in Cyberspace global initiative led by the GCF, which is taking action to ensure a safe and empowering Cyberspace for children around the world. GCF's leadership and vision for this initiative continue to advance global efforts on child cyber protection, shaping the strategic mission that informs these Principles.

ITU and the SRSG-VAC extend their sincere appreciation to all those who contributed to and supported the development and validation of the PoP guiding principlesPOP, as well as to the children and young people whose perspectives continue to inspire this work.

Participation in the PoP initiative or contribution to this publication does not imply endorsement, in part or in full, of its contents by any participating organization.

In partnership with:

Table of contents

Foreword

Executive summary

Protection through Online Participation (PoP) is a global, multi-stakeholder initiative co-led by the Office of the Special Representative of the United Nations Secretary-General on Violence Against Children and the International Telecommunication Union. It aims to ensure children can safely access protection and support through digital platforms, when at risk of experiencing any form of harm, both in person and online.

Recognizing the dual nature of the digital environment, as both a space of risk and a gateway to safety, PoP introduces **five guiding principles (5Ps)** to help policymakers, technology platforms, and child helplines and similar services transform digital spaces into protective infrastructures:

1. **Protect** – Prioritize safety, inclusivity, and accessibility in digital services.
2. **Progress** – Expand and diversify digital strategies to support children.
3. **Partner** – Foster multi-stakeholder collaboration for child protection.
4. **Participate** – Engage children meaningfully and safely in shaping digital solutions.
5. **Push** – Advocate, invest, and innovate to strengthen digital protection systems.

These principles are **voluntary and aspirational**, grounded in child rights frameworks and designed to complement existing international efforts. They call for a **holistic, rights-based approach** that integrates digital pathways into broader child protection systems.

Insights from child helplines, technology platforms, and children themselves confirm that digital tools, when designed ethically and inclusively, can enhance access to timely, confidential, and effective support. However, challenges remain, including data privacy, accessibility, and resource constraints.

Moving forward, PoP urges stakeholders to:

- Embed protection mechanisms within platforms children already use.
- Invest in inclusive technologies and digital literacy.
- Promote child-led innovation and participation.
- Strengthen evidence-based approaches and cross-sector collaboration.

By adopting the PoP guiding principles, stakeholders can reimagine the digital environment not just as a space to regulate, but as a **lifeline for children's protection, support, and empowerment**.

PART ONE – The 5Ps

Introduction

Facilitating children access to protection and support through digital technologies

Although approximately one billion children, between 2 and 17 years of age, are thought to have experienced physical, sexual, or emotional violence or neglect within the past year,[1] violence against children often remains hidden. As traditional analogue services are not always accessible, or within reach of children, many children still face barriers to reporting harm. In such contexts, where connectivity is available, digital tools, developed with child rights and safety in mind, can be lifesaving, by offering avenues for children to connect with protection and support.

The digital environment[2], offers immense opportunities for children to learn, create, and connect, but also increasingly exposes them to a wide range of online risks. These risks are evolving rapidly, driven by emerging technologies such as artificial intelligence, immersive virtual environments, and algorithm-driven platforms. Consequently, global efforts are underway to make the Internet safer for children through policy reforms, technological safeguards, educational initiatives, and child-centred design. Legal and policy frameworks are central to strengthening child online protection, and promising practices already exist that can serve as valuable models.[3]

Preventing and addressing online violence against children requires continuous, coordinated action grounded in a holistic, rights-based approach.

At the global level, initiatives such as the Global Digital Compact are advancing digital cooperation and frameworks, and promoting responsible, protective and inclusive uses of emerging technologies, as well as cross sectoral collaboration on digital governance. Only through sustained, multi-stakeholder collaboration can a digital ecosystem evolve where children are truly safe, empowered, and protected from harm.

Making the Internet safer for children requires a comprehensive approach to both preventing and responding to violence. This includes the active removal of harmful content that violates children's rights, accessible and effective reporting pathways, and the proactive identification of other opportunities to further strengthen child online protection, through innovation, regulation, capacity-building, and collaboration. Digital platforms could play an active role in enhancing child online protection, including facilitating connections to child helplines and similar services,

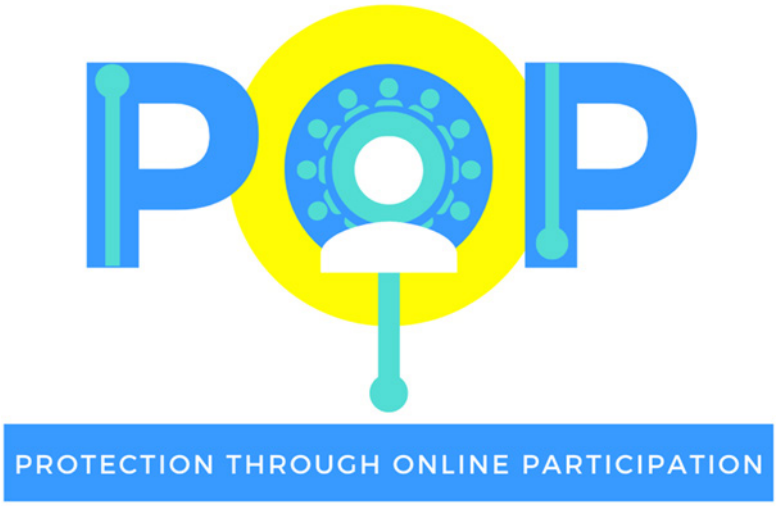
---

1 https://www.who.int/teams/social-determinants-of-health/violence-prevention/online-violence-against-children

2 General Comment No. 25 defines the digital environment as *the totality of digitally networked spaces, services, and technologies that children access and interact with, including the Internet, social media, apps, and connected devices.*

3 **Frameworks and guidance:** ITU *Child Online Protection Guidelines*; UNICEF *Global Guide on Legislating for the Digital Age*; AU *Model Law on Child Online Safety*; OECS *Child Online Protection Framework*; ASEAN *Regional Plan of Action (2021–2025)* and *Guidelines (2023)*. **Legal and regulatory instruments:** United States of America *COPPA* and *CIPA*; United Kingdom *Online Safety Act (2023)*; European Union *Digital Services Act* and *Guidelines on the Protection of Minors (2025)*; proposed European Union *Regulation on Preventing and Combating Child Sexual Abuse*; European Union *Cyber Resilience Act (2024)*; *Jutland Declaration*; European Union *prototype age-verification app* and *Digital Identity Wallet*; emerging national laws on age verification, device bans, and online safety awareness.

and enabling digital spaces to serve as gateways to safety and assistance. In this way, digital platforms could help to protect children's rights through the provision of a secure, inclusive, and empowering online environment.



The digital environment therefore presents a dual reality for children: while it can expose children to harm, it also holds the transformative potential to connect children with safety, protection, and support. Recognizing this, the Office of the Special Representative of the United Nations Secretary-General on Violence Against Children (OSRSG-VAC) and the International Telecommunication Union (ITU) have co-led the Protection through Online Participation (PoP) initiative aimed at ensuring children can safely access help through digital means. PoP is a global, multi-stakeholder initiative that leverages technology-enabled systems such as child helplines and similar services, to expand the global understanding of online safety and promote the use of digital platforms as pathways to child protection and support. When experiencing any form of harm, whether in person or online, children should be able to use digital platforms to connect with safety and protection.

To unlock the potential of digital technology to help children in a safe and inclusive manner, PoP promotes a coordinated, rights-based approach, where diverse stakeholders work together to embed online safety within broader child protection systems and digital development strategies. The PoP initiative brings together about 30 partners, including United Nations agencies, civil society organizations, child helplines, technology companies, academia, policy-makers, and children themselves. Collectively, they have developed five guiding principles that can be applied to reimagine the digital environment not just as a space to be made safer, but as a vital point of access to protection and support.

The 5Cs framework, which considers online **content**, **contact**, **conduct**, **contract**, and **cross-cutting** risks, is used to classify the diverse and evolving risks children face in digital spaces. However, these online risks are deeply intertwined with the harm children experience offline, such as violence, exploitation, discrimination, and exclusion. Building on this understanding, PoP has introduced five guiding principles, referred to as the 5Ps to guide different stakeholders when connecting children with protection and support through digital means: **protect**, **progress**, **partner**, **participate**, and **push**. The 5Ps are intended to guide a strategic and participatory approach towards making the Internet safer by suggesting ways forward for policy-makers, technology platforms, and child helplines. The goal is to facilitate access to protection and support through digital platforms, for children who are at risk of experiencing violence, whether

online or offline. The 5Ps emphasize the need for action that is not merely confined to the digital ecosystem, but that is also grounded in broader child protection systems and rights-based frameworks. To truly safeguard children, we must reject the notion of the Internet as a separate sphere and instead embrace integrated, multi-stakeholder efforts that address the full continuum of risks and opportunities across both online and offline environments.

The digital environment is complex and constantly evolving, and stronger efforts are needed to make it safer for children. PoP broadens the global understanding of online safety by highlighting the potential of technology to connect children with protection and support. Though facilitating access to these services is a vital step toward a safer Internet, the challenge is multifaceted and demands a more comprehensive approach that addresses all dimensions of child protection, both online and offline.

Anchored in the United Nations Convention on the Rights of the Child, and including its three Optional Protocols, as well as a number of other relevant human rights treaties, and in alignment with General Comment No. 25 on Children's Rights in the Digital Environment, the 5Ps are grounded in a shared commitment to upholding children's rights, including their safety, privacy, and well-being. The principles adopt a child-rights-centred approach, offering a principled and evidence-based framework to assess and respond to the interplay between children's rights to provision, protection, and participation. This approach enables governments, civil society, businesses, educators, researchers, and caregivers to weigh the risks of harm originating online, while recognizing the meaningful opportunities and benefits digital engagement can offer children and their families.

These guiding principles are advisory in nature and are intended to encourage policy-makers, digital technology companies, civil society organizations, child helplines, and similar services to use digital technologies to prevent, address, and respond to violence against children.

They are also aspirational, aiming to foster a more holistic approach to child protection in the digital environment. This means not only ensuring that children are safe from online harm but also enabling digital platforms to serve as gateways to protection and support regardless of the nature of the risk. A comprehensive approach to online safety recognizes the digital world as both a space to be safeguarded and as a tool for enhancing children's overall safety.

The 5Ps are positioned as complementary to existing international frameworks on online safety and children's rights in the digital environment. They can be adopted or integrated in alignment with broader global frameworks, helping to avoid duplication and promote coherence. Practical pathways for endorsement include the adoption of voluntary codes of conduct, integration into national strategies, and alignment with broader online safety and child protection frameworks.

The 5Ps reflect the responsibility of all stakeholders to keep children safe from harm, but are particularly intended for consideration by the following three key actor groups who play a vital role in enabling children to safely seek and receive support through digital means:

Policy-makers are responsible for ensuring, through national policies, legislation, and strategies, that their approach to children's protection incorporates digital pathways for children to access protection and support. Their role also includes providing sustained support to services working to safeguard children.

Digital technology platforms are well positioned to facilitate access to protection services, such as child helplines, and to help detect harm before it occurs by supporting risk prevention

efforts. Digital platforms can foster supportive communities, promote help-seeking behaviours and support for children, and strengthen the role of the digital environment as an entry point to access safety and protection

Child helplines and similar services are the frontline providers of support to children at risk, often operating 24/7 through multiple digital channels, and are recognized as an entry point to national child protection systems. Their work is essential in ensuring that children receive timely, appropriate assistance when facing harm.

The 5Ps also apply to a broader range of child-facing actors such as educators, and cultural, religious, and sports organizations.

The five guiding principles are grounded in the insights and practical experiences of a wide range of stakeholders. To develop the guiding principles, PoP drew upon the lessons learned and knowledge shared by child helplines and similar online support services, technology companies, policy-makers, and crucially, children and young people themselves. Their perspectives and experiences helped shape the development of the 5Ps and are further elaborated in Part Two of this document.

These guiding principles help chart a path toward a digital ecosystem where children's rights are not only protected but actively promoted. They encourage all actors to reimagine the digital environment, where a safer Internet also means safer ways to access help.

The 5Ps for protection and support

To enable children to access protection and support through digital means, policy-makers, digital technology platforms, and child helplines and similar services should consider the five guiding principles, as outlined in Table 1.

Table 1: 5Ps

1 **Protect**	2 **Progress**	3 **Partner**	4 **Participate**	5 **Push**
Prioritize safety, inclusivity, and accessibility	Expand and diversify actions and strategies to protect and support children	Team up. Collaboration is the secret of success	Engage the experts. Meaningfully and safely engage children and youth	Commit and advocate to help children access protection and support through digital platforms

This section outlines each of the five guiding principles and the particular relevance of each to policy-makers, digital technology platforms, and child helplines and similar services.

1 - Protect: Prioritize safety, inclusivity, and accessibility.

Policy-makers

Facilitate the creation of a safe and enabling environment through which children can access safety and protection through digital means, recognizing that online and offline experiences are interconnected and inseparable in children's lives.

- Protect children's safety: National strategies to prevent violence against children should establish robust legal, regulatory, and policy frameworks to ensure, support and promote the safe operation of child helplines and related online services, including any digital channels children use to seek help. These frameworks should address data protection, operational procedures tailored to digital environments, and safeguards for children's privacy and safety[4].
- Protect child sensitive digital referrals: Referral mechanisms supported by online child helplines (including emergency services, health services, and legal aid services) should include digital tools that are easy and safe for children to use. These tools need to be backed by strong policies that ensure services follow national safety standards and work properly, protect children's personal information, and are reviewed regularly to stay up to date with current best practices.
- Protect children through equitable access to services: Services should be made accessible to all children, 24/7, including marginalized groups, children with disabilities, and those in remote areas, while ensuring their safety when using digital reporting platforms.

Digital technology platforms

Ensure safety within your platforms, including when children use them to access protection and support.

- Protect children's safety: Commit to adhering to the highest standards of privacy and safety, including a safety-by-design approach[5], in relation to the design, engineering, development, operation, distribution and marketing of products and services. When children use technologies to access protection and support, ensure age-appropriateness and accessibility.

---

[4] The policy frameworks should reference guiding principles such as safety and privacy by design, and internationally validated recommendations such as the ITU COP Guidelines.

[5] Safety by Design principles refer to proactive approaches that embed child safety and user protection into the design, development, and deployment of digital products and services. Rather than relying solely on reactive measures, these principles ensure that safety features are integrated from the outset, minimizing risks and promoting responsible innovation. They are especially important in creating online environments that are safe, inclusive, and age-appropriate.

- Protect children's data: Uphold legal and ethical data best practices. When facilitating access to digital channels to support children, establish clear and ethical guidelines for data handling, ensuring compliance with data protection regulations.
- Protect together: Include relevant stakeholders, such as civil society organizations, academia, experts on protection, government, children, child helplines, and similar services in an advisory capacity to ensure needs are met and appropriate safeguards are in place.

Child helplines and similar services

Ensure that digital channels are safe for all children to use

- Protect children's safety: Ensure digital channels are safe for children to use, and to provide feedback on, by incorporating intuitive and accessible safety features, and by applying the highest safeguarding standards, taking into account children's level of maturity and development.
- Protect children's personal information: Uphold ethical data protection practices. When incorporating digital channels to support children, establish clear and ethical guidelines for data handling, ensuring compliance with data protection regulations.
- Protect children through equitable access: Always aim to improve the accessibility and resilience of online support services, ensuring they are easily accessible to all children, including children with disabilities, those with limited bandwidth, in rural areas and during emergency situations. Ensure communication remains available when disruptions occur.

2 - Progress: Expand and diversify actions and strategies to help and support children.

Policy-makers

Progress by enabling access. Create environments where children can access protection and support through diverse channels. Expand and strengthen national strategies to prevent and respond to violence against children, by integrating digital pathways for safety.

- Progress by protecting: Expand approaches to children's protection by creating forward-looking policies that facilitate the expansion of child helplines into inclusive, digital support systems. This includes promoting the use of webchat, mobile apps, and social media to reach children who may not engage with traditional helplines. Policies should also ensure funding and technical support to scale and sustain these services.
- Progress through safe technologies: Promote technologies that help children access safety and protection services. Policies should incentivize tools that detect, prevent, and report harm, and connect children to protection services safely and effectively.

Digital technology platforms

Adopt a broader, more comprehensive understanding of safety, that facilitates children's access to protection and support through digital platforms.

- *Progress by preventing harm*: Use technology to detect early risk signals, guided by child rights, due diligence, and impact assessments, and connect children to timely support such as helplines and similar services.
- *Progress by responding to harm*: Optimize sector-wide opportunities for children and young people to access protection from online and offline violence through development of timely and safe support services.

Child helplines and similar services

Progress by expanding and diversifying channels to incorporate safe online support systems that effectively counsel and support children and young people.

- *Progress by expanding support*: Continue to diversify access channels in a meaningful way, by evaluating the advantages of integrating digital platforms into your service. Identify which online spaces are most commonly used by children and young people, how they access them, and on which topics children seek help through online means.
- *Progress by meeting diverse needs*: Support multiple communication channels simultaneously and tailor counselling options for each, whether through trained peers, professional counsellors, or blended approaches, to ensure every child can access support in the way that best meets their needs.

3 - Partner: Team up. Collaboration is the secret to success.

Policy-makers

Encourage and convene multi-stakeholder partnerships for children to get the protection and support they need through digital platforms.

- *Partner for digital protection*: Governments should establish strategic partnerships among technology platforms, child helplines and similar services, and public institutions to enhance digital access to protection and support, ensuring a coordinated, cross-sectoral response to violence against children.
- *Partner for digital innovation:* Governments should promote public-private partnerships that drive technological innovation to expand social protection systems and develop effective digital platforms for child-focused support services, including child helplines and similar services.

Digital technology platforms

A collective approach is a successful approach. Partner with others, and with each other.

- *Partner for digital protection*: Foster strategic intersectoral collaboration to promote the power of technologies to support children. Partner and collaborate with public entities, protection stakeholders, child helplines and similar services, and children and youth-led initiatives, who can directly help and support children experiencing any form of harm.
- *Partner for digital innovation*: Participate in collaborative actions. Join collective efforts and proven solutions to advance and respond to the use of technologies as a channel to connect with assistance and support.
- *Partner for collective impact*: Grow together. Share insights, knowledge, proven solutions, and lessons learned within the sector on how technologies are used to connect children with protection, including the use of technologies in detecting and responding to harm.

Child helplines and similar services

A collective approach is a successful approach. Foster intersectoral partnerships.

- *Partner for protection*: Collaborate with different stakeholders, including government, law enforcement, civil society organizations, telecommunication operators, technology companies, children and young people, and other relevant entities to develop and expand online support services.
- *Partner for collective impact*: Engage in collaborative thinking. Share data, good practices, insights and learnings to constantly improve ways of providing children with protection and support through online means and ensure these collaborations are framed within clear protocols and safeguards.
- *Partner for digital innovation*: Partner with digital technology companies. Strive for direct collaboration with companies behind online spaces used by children in your country. Jointly implement online support systems leveraging innovative technology and resources, ensuring accessible, secure, and child-friendly support for those in need.
- *Partner with each other*: Join networks of child helplines and similar services, and use the platforms offered to share good practices, innovations and experiences in working with digital technology.

4 - Participate: Children are the first experts. Meaningfully and safely engage children and young people.

Policy-makers

Promote and encourage children's meaningful and safe participation at all stages of child protection processes.

- *Protect through participation*: Policy-makers should actively and meaningfully involve children in shaping the policies, technologies, and services that affect children's safety and well-being[6]. This includes co-creating solutions with children at every stage of the process and encouraging the private sector to do the same, ensuring children's experiences, insights, and calls for change are heard without compromising their privacy or safety.
- *Power participation for change*: Policy-makers should encourage and support child-led initiatives to prevent and report violence. This includes empowering children to take action and ensuring their safety and timely access to appropriate services.

Digital technology platforms

Your users know best.

- *Protect through participation:* Learn from child and youth-led solutions that address protection through digital technologies, including peer to peer approaches, community support groups inside your platforms, and others.
- *Position participation in technology for protection*: Meaningfully and regularly engage with children and young people around designing and evaluating ways of using digital technologies as channels to connect with assistance and support services concerning their protection and wellbeing.

Child helplines and similar services

Recognize children's significant role and perspective within online services.

- *Promote participation throughout the process*: Involve children in the design and decision-making processes of online support systems to ensure alignment with children's needs and preferences. Their input should also be sought in evaluating service and interaction quality to enhance user experience.
- *Promote participation in service feedback*: Continue to develop transparent user evaluation frameworks, incorporating factors such as accessibility, responsiveness, and user satisfaction, ensuring accountability and continual improvement in service delivery.
- *Protect through participation:* Foster children's capacities to provide peer-to-peer support, ensuring safeguards and adult support.

---

[6] *Article 12 of the UNCRC* affirms the right of every child to express their views freely in all matters affecting them, with those views given due weight in accordance with the child's age and maturity. Meaningful participation is a cornerstone of child rights and is essential in shaping policies, technologies, and services that impact children's safety and well-being.

5 - Push: Commit, advocate, and invest in digital platforms that protect children, supporting prevention, detection, and response to violence as a foundation for building human capital.

Policy-makers

Push for investment, innovation, informed access, and evidence-driven ethical, child-centric digital solutions that protect and empower children through inclusive infrastructure, education, and ongoing research.

- *Push for investment*: Encourage sustained investment in child protection through digital infrastructure and AI-driven services that ensure timely, accessible, and effective support.
- *Push for capacity*: Strengthen the capacity of all actors involved in child protection, including but not limited to frontline workers, practitioners, counsellors, educators, law enforcement officers, judicial and healthcare professionals, ICT specialists, and community-based organizations.
- *Push for innovation*: Leverage AI and emerging technologies to create ethical, child-rights respecting tools for protection and support, such as real-time risk detection and safer reporting, supported by inclusive infrastructure and digital literacy skills.
- *Push for informed and safe access*: Provide child-centric educational resources and digital literacy programmes for children, families, and educators to safely access online support services. Promote awareness of child helplines and digital tools, tailored to children's developmental needs, to empower their use of technology for protection and support and foster a help-seeking reporting culture among children and adults.
- *Push for evidenced-based solutions*: Encourage research on how effective digital tools are in helping children access protection and support when facing harm online or offline.

Digital technology platforms

Commit and advocate: Digital technologies can help children access protection and support.

- *Push for investment*: Invest in children's safety, by allocating appropriate resources to support systems available to children to access protection and support when using digital platforms.
- *Push for evidence of impact*: Assess the impact of your organization's approach to children's access to protection systems through digital technologies. Develop metrics that show how your platforms are helping facilitate children's access to protection and support.
- *Push for team engagement*: Involve your colleagues. Be an advocate for children's protection inside your company, by raising awareness and empowering your colleagues to fully understand the positive impact your technologies can have on children's access to protection and support.
- *Push for more*: Be a champion in the sector. Advocate for the power of technologies to bridge children with protection and support.

Child helplines and similar services

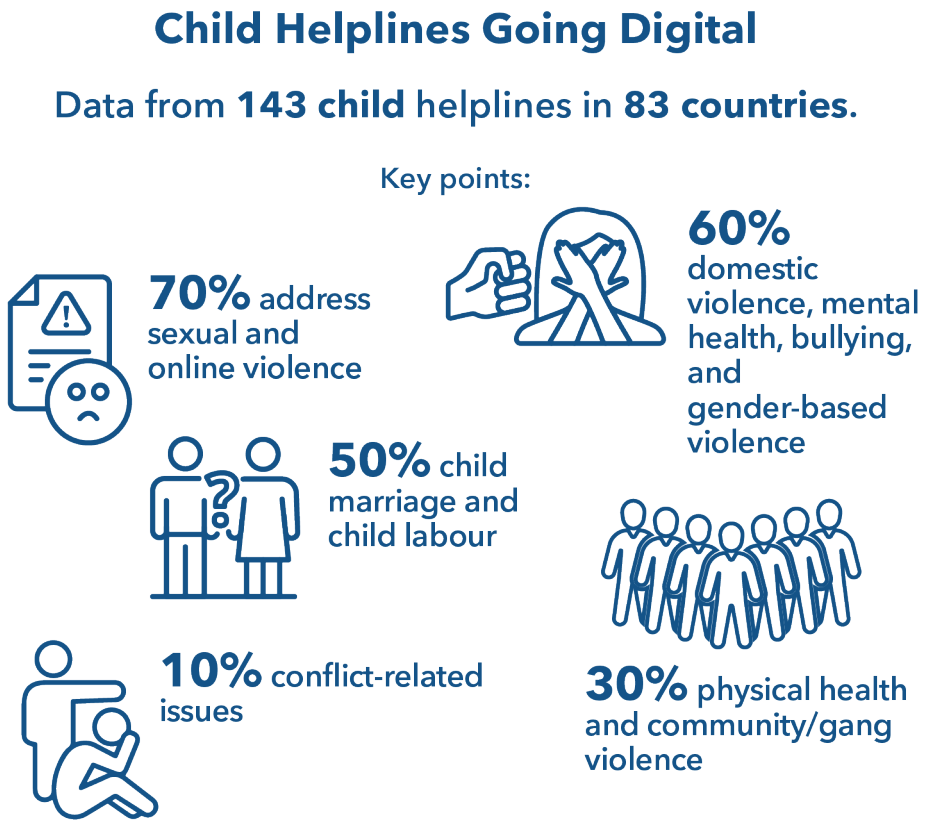
Use digital channels to advocate for further commitment.

- *Push for data-informed protection*: Use digital technologies to collect metrics, conduct analysis and collate actionable evidence. Use this data to inform child protection programmes and policies, and to advocate for further investment in children's protection and wellbeing.
- *Push for frontline experts:* Build the digital capacities and skills of counsellors and practitioners, to be able to respond to children's protection needs through online channels.
- *Push for collaboration*: Foster holistic collaboration by sharing your expertise to strengthen technology platforms that support children's access to protection and care.

PART TWO – Insights from data collection

Data-driven development of the 5Ps

To better understand how children are using digital platforms to access protection and support, PoP collected insights and perspectives from key stakeholders. These insights informed the development of the 5Ps. The following section summarizes the insights collected and the processes through which they were obtained. This section is not intended to be an exhaustive analysis of how digital platforms are used by children to access safety and protection; rather, it offers a reflection of the perspectives and insights shared by the organizations consulted.



Child helplines going digital

PoP conducted a global mapping of in-country services using Internet-based systems to support and counsel children. Data was gathered through an online survey capturing insights on service types, technologies used, communication channels, forms of violence addressed, and the benefits and challenges of online child protection systems.[7] A total of 143 child helplines and

[7] The information provided in the survey was self-selected and should not be viewed as globally or regionally representative.

similar services from 83 countries[8] shared valuable insights, highlighting the diversity and adaptability of online child protection systems. Key findings are summarized below.

Most of the services consulted are operated by civil society organizations, followed by government-run initiatives. Their primary functions include offering counselling, receiving reports of violence, and providing information for children, young people, girls, and women. In most countries, child helplines use multiple communication channels and telephone remains the most widely used, while online platforms often serve as complementary tools. Some services, however, were established entirely online and continue to operate exclusively in that space.

These online channels address a broad range of risks, not limited to Internet-related harms. Over 70 per cent of services support cases involving sexual and online violence; over 60 per cent address domestic violence, mental health, bullying, and violence against girls and women; more than 50 per cent deal with child marriage and child labour; over 30 per cent cover physical health and community or gang violence; and over 10 per cent respond to issues related to armed conflict.

Users engaging through online platforms can interact with a variety of responders, including child protection professionals, social workers, mental health specialists, and peers. Peer-to-peer support and mental health services were particularly prominent in some regions.

In terms of technology, service providers favour platforms that support multiple forms of communication, such as instant messaging, social media, and gaming platforms, and webchat.

How digital technologies strengthen child helplines

Versatility and user-centred design

Digital platforms and services via apps, web portals, messaging, or social media can offer flexibility in how children and young people access support. Where available, users may choose the channel and interaction style that best suits their needs, whether one-on-one with a counsellor, peer support, or moderated group discussions. Unlike voice calls, online platforms can allow for simultaneous, multi-user interactions. These channels can also meet children where they are, online, offering a sense of privacy, anonymity, and comfort, that is especially important when dealing with sensitive issues such as violence or mental health.

[8] Republic of Albania, People's Democratic Republic of Algeria, Republic of Azerbaijan, Kingdom of Bahrain, Belgium, Bosnia and Herzegovina, Republic of Botswana, Federative Republic of Brazil, Republic of Bulgaria, Burkina Faso, Kingdom of Cambodia, Canada, Chile, People's Republic of China, Republic of Colombia, Costa Rica, Republic of Cyprus, Denmark, Dominican Republic, Republic of El Salvador, Federal Democratic Republic of Ethiopia, Finland, France, Republic of the Gambia, Ghana, Greece, Republic of Guatemala, Republic of Guinea, Hungary, Republic of India, Ireland, Italy, Republic of Côte d'Ivoire, Jamaica, Japan, Republic of Kazakhstan, Republic of Kenya, Republic of Palau, Lebanon, Republic of Lithuania, Republic of Mali, Malta, Republic of Mauritius, Mexico, Republic of Moldova, Kingdom of Morocco, Republic of Mozambique, Republic of Namibia, Kingdom of the Netherlands, New Zealand, Republic of the Niger, Federal Republic of Nigeria, Norway, State of Palestine, Republic of the Philippines, Republic of Poland, Portugal, Romania, Republic of Rwanda, Saint Vincent and the Grenadines, Kingdom of Saudi Arabia, Republic of Serbia, Sierra Leone, Slovak Republic, Republic of Slovenia, Republic of Korea, Spain, Sweden, Confederation of Switzerland, Syrian Arab Republic, Taiwan - Province of China, United Republic of Tanzania, Thailand, Trinidad and Tobago, Republic of Türkiye, Republic of Uganda, Ukraine, United Arab Emirates, United Kingdom of Great Britain and Northern Ireland, United States of America, Socialist Republic of Viet Nam, Republic of Zambia

Efficiency in support and case management

When available, online systems enable longer, more flexible conversations, than traditional telephone voice calls, allowing users to pause and resume conversations without losing continuity. Counsellors can access conversation histories, share resources in real-time, and manage multiple cases simultaneously. These online systems also offer counsellors flexibility in terms of providing remote support, enabling these services to run across different times. While helplines may have concerns about data privacy, some[9] use AI to help identify and prioritize urgent cases. Digital tools also streamline internal coordination, profile management, and secure data sharing, enhancing service quality and responsiveness.

Expanding reach and strengthening advocacy

Digital channels can broaden outreach and enable helplines to serve and support more users efficiently. They make real-time referrals possible, reduce operational costs, and facilitate data collection on children's needs and experiences. This anonymized data, combined with increasingly AI-enabled analysis can inform the development of programmes, policies, and advocacy efforts, provided it is managed with strong privacy safeguards and child protection standards.

Unpacking the challenges of digital child helplines

Challenges affecting the users of child helplines

Exposure to online risks: While digital platforms offer access to support, they also expose children to the digital environment, and therefore potentially to online harms.

Protecting children's data and privacy: Digital support platforms expose children to the digital environment, and therefore to the associated challenges of protecting their data and privacy. Helplines must balance accessibility with safeguarding privacy and data, especially when using third-party platforms such as social media sites or gaming apps.

Loss of non-verbal cues: Most digital systems used by child helplines to support children and young people are text based and lack tone and body language, making it harder for counsellors to assess emotional states or detect distress, which can hinder timely interventions.

Sustaining engagement: Digital platforms allow users to drop in and out. While depending on the child, this may be an advantage, it may equally make it difficult to maintain consistent conversations and communication. Children may be disengaged for various reasons and may not return.

Limited access: Not all children have reliable access to digital devices, data, or Wi-Fi. Barriers such as gender norms, cultural factors, cost, and availability of technology can limit access to online child support.

[9] Some stakeholders opt to negotiate zero-data-retention agreements with AI systems or choose open-source solutions to ensure that sensitive data remains securely within the helpline infrastructure.

Challenges affecting child protection organizations

Resource demands: Adding digital channels increases operational costs in terms of technology development, maintenance, staff training, and scaling of personnel to meet rising demand.

Customization needs: Digital tools must be adapted to diverse user needs, including multiple languages, and accessibility for children with disabilities. A one-size-fits-all approach is ineffective.

Data and platform limitations: Some technology platforms used by children to connect with protection and support may compromise privacy, and child helplines must navigate these risks while ensuring safe, ethical engagement.

Digital technology as a gateway to protection: Insights from social media and gaming platforms

PoP gathered insights from social media and gaming platforms to understand how children use digital spaces to seek safety and support. Findings show that children frequently turn to these platforms when facing or fearing harm, especially from bullying, cyberbullying, mental health issues, sexual violence, and domestic violence. Social media and gaming platforms can often serve as access points to other sources of protection and support.

Children sometimes connect with support services through in-platform help centres, links to child helplines or peer communities, or by searching for relevant information. Many platforms are responding by partnering with child helplines, integrating crisis response tools, using trusted flaggers, and embedding safety content directly into user experiences, though this in some cases lacks consistency and strategic planning.

What is working well

Cross-sector collaboration has helped extend the reach of child protection services, with digital technology platforms partnering with child helplines and directing or signposting users to connect with child protection services when needed. Local partnerships help and enable global platforms to connect children with country-specific child protection services.

Digital technology can also enable early detection of risks and can allow support to be both personalized and anonymous within online spaces that children use daily. It can also help disseminate protection-related content to help prevent harm before it occurs.

Peer support communities within platforms are valuable for mental health and discrimination-related issues.

Challenges to be addressed

Audience-related challenges

Flexible, multi-lingual and multi-device: Children use a wide range of platforms, devices, and languages, making it essential to offer flexible, multi-channel solutions that can function across different technologies and devices and are accessible in multiple languages.

Protecting privacy in sensitive digital spaces: Privacy is a major concern when addressing child protection issues, particularly relating to the collection and use of children's personal data when child helplines and similar services operate on these platforms to support children.

What does 'help and support' mean: The definition of 'help and support' varies significantly, requiring approaches that can adapt to children's diverse needs and expectations.

Challenges when partnering

From global to local: The problems are global, but the solutions are local. Global platforms should partner with child helplines and similar services to refer cases locally to meet child protection needs, however identifying appropriate services in each country can be complex.

When demand may exceed capacity: Technology platforms are concerned that local services might lack the capacity and resources to manage increased demand generated from platform referrals.

Internal challenges of digital platform companies

Clarifying internal responsibility for connecting children with digital protection services: Many digital platforms struggle to determine which internal team should be responsible for connecting children with protection and support, especially when the harm experienced is not directly linked to online activity, as conventional Trust and Safety frameworks typically mandate companies to address the harms resulting from their own services.

Overcoming internal challenges for technology integration: On a technical level, insights indicated that some companies are faced with complex technical integrations when connecting children with external child protection services, such as child helplines. This may require integrating these external services into the platform to enable direct counselling, requiring ongoing evaluation to ensure effectiveness. Legal, financial, and procedural barriers can further complicate the incorporation of child helplines and related protection services into platform infrastructure.

Children and Young People's Views

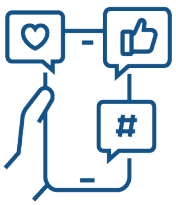
Based on an online poll with ~600 participants from 87 countries.

76% said they turn to online platforms for support.

Where they seek help:

33%
child helplines

27%
messaging apps



24%
social media

Digital platforms as a gateway to safety: Insights from children and young people

PoP collected insights from children and young people on how they use digital platforms to access safety and protection, through an online poll[10] and in-depth interviews with young people who have been leading the development of digital solutions for their peers to access safety and protection. The online poll engaged nearly 600 children and young people across 87 countries to explore their help-seeking behaviours when feeling uncomfortable or unsafe. A majority of 76 per cent reported turning to online platforms for support either always or sometimes. When asked where they specifically seek help, most indicated online child helplines (33 per cent), messaging Apps (27 per cent), and social media platforms (24 per cent).

In-depth interviews with young people who have developed diverse online solutions for their peers to access safety and support [11], further confirmed that children and young people are increasingly turning to digital environments not only for connection and learning, but also as vital avenues for accessing protection when facing risks of harm, either online or in person. Some youth-led solutions[12] go beyond awareness-raising to provide interactive tools, safe spaces, and peer-led mechanisms that help children recognize risks such as online scams, misinformation, grooming, or unsafe interactions. Crucially, these solutions are also designed to facilitate access to official sources of help, including helplines, referral services, and in-app emergency support features. Through simulations, training modules, and peer-to-peer exchanges, young people are empowering their peers not only with knowledge but also with concrete pathways to seeking protection and support when needed.

Effective solutions powered by young people

According to the young people who have developed some of these solutions and were interviewed, providing protection and support via online means is particularly effective because of the anonymity, accessibility, and youth-led development (given that children and young people understand the needs of their peers). Young people feel more comfortable seeking help when they can do so privately, without fear of exposure or judgment. Text-based support, peer community forums, and youth ambassadors also help to bridge the gap between children in need and the services available to them.

Major challenges faced by young people when developing solutions

However, despite their positive impact, developing and implementing these youth-led solutions comes with significant challenges, such as the difficulty for young people to design content that is accessible and engaging across a broad age range, from younger children to older teens. Additionally, while some of these youth-led solutions aim to foster dialogue, they often lack the infrastructure to host open discussions about online risks. This can potentially expose

---

10 This online poll was disseminated in February 2024, and asked children and young people if when feeling unsafe or uncomfortable they looked for help online. This period preceded the rapid expansion of artificial intelligence systems and did not specifically address AI modes of engagement.

11 PoP interviewed young people leading the following initiatives: Masterclass (Your life online: be safe, be empowered), Ethesab, and children from the Childnet advisory board.

12 In this document, "child- and youth-led solutions" refers to initiatives, tools, and safe spaces created or shaped by children and young people themselves. These may include peer-to-peer networks, apps, interactive platforms, or community-based groups that provide guidance, information, or pathways to support. While not formal child protection services, such solutions often act as bridges, linking peers to official systems (e.g. helplines, hotlines, counselling) or informal networks of care and assistance.

children to risks[13], such as misinformation and disinformation, harmful content, public or private oversharing of personal information, radicalization, and various forms of violence, including domestic abuse and grooming.

Youth-led structures, though empowering, can struggle with continuity, coordination, and visibility, especially in crisis contexts, due to limited funding and support. In some countries, young developers face political constraints, safety risks, and limited access to funding or partnerships. Some may even need to operate underground, relying on trust-building and phased scaling to avoid shutdowns. The digital divide also remains a concern, leaving children without access to devices or connectivity means they remain excluded from accessing child protection resources. Finally, while young people consulted felt that the issue of online safety concerns is relatively well-covered, they felt that providing guidance for children on what to do when facing offline harm remains a challenge.

These challenges highlight the need for inclusive, adaptable, and well-supported digital environments that can truly serve as protective infrastructures for all children and young people.

Advancing digital safety and protection for children and young people

Children's interactions with the digital world are dynamic, multifaceted, and deeply connected to their experiences of safety and protection, including the support they can access online. Digital platforms are not only spaces where children may face risks, but are also important gateways to care, connection, assistance and support, often shaped by children themselves in innovative ways.

The guiding principles presented in this document acknowledge this dual reality and call for a paradigm shift in perspective: moving from viewing the digital environment solely as a space to regulate, toward recognizing its potential to be purposefully designed and leveraged to uphold children's rights.

These five guiding principles are voluntary and aspirational. They invite all stakeholders including policy-makers, technology platforms, civil society, and service providers, to move beyond minimum standards and reimagine child protection for the digital age. They advocate for a holistic approach where digital spaces are not only safe but also serve as trusted avenues for accessing protection and support. Prevention, response, and recovery mechanisms should be embedded within the platforms children already use and rely on.

Looking ahead, sustained advocacy is essential to ensure that every child can access these vital digital lifelines. Realizing the full potential of technology to protect children requires a coordinated, multi-stakeholder approach, one that brings together governments, technology companies, child protection services, civil society, and children themselves. This includes investing in violence prevention, strengthening child helplines, and developing ethical, inclusive technologies that safeguard privacy and data rights. In addition to protection, stakeholders who design and operate digital platforms and services should promote resilience, strengths-based

[13] Online risks are referred to in this context as per the 4Cs framework, which categorizes risks children face in digital environments into four key areas: **Content** (exposure to harmful or inappropriate material), **Contact** (interactions with potentially harmful individuals), **Conduct** (children's own behavior online, including cyberbullying or risky sharing), and **Contract** (risks related to commercial exploitation, such as misuse of personal data or hidden costs). This framework is widely used to guide child-centred digital safety strategies.

development, and positive childhood experiences, recognizing that technology is a tool, and its impact depends on how people design and use it.

Children must be meaningfully involved in shaping these solutions. Their participation in the design, implementation, and evaluation of digital tools ensures that interventions are relevant, effective, and grounded in lived experience. Equally important are sustained education and awareness efforts targeting children, caregivers, educators, and service providers to promote safe digital engagement and informed use of support services.

Finally, advocacy must champion research and evidence-based approaches to monitor and evaluate digital protection efforts. Only through continuous learning and adaptation can we ensure that digital technologies truly serve the best interests of children, offering not just access to help, but confidence in their safety, support, and well-being in an increasingly connected world.

These guiding principles complement existing international frameworks on online safety and children's rights in the digital environment. Rather than replacing current efforts, they aim to enhance them, through collaboration, innovation, and a child rights-centred approach. The guiding principles are intended to evolve through consultation and periodic updates to maintain relevance.

These guiding principles can be adopted or integrated in alignment with broader global frameworks, helping to avoid duplication and promote alignment. Practical pathways for endorsement may include voluntary codes of conduct or integration into national strategies or other related frameworks.

Protecting children online is a shared responsibility. With these guiding principles as a foundation, and with accountability across all stakeholders, we can work together to ensure that digital platforms and services contribute to children's protection, not only shielding them from harm, but also empowering them to seek help, access the services they need, and thrive.

Glossary of digital terms

- **digital environment**: The totality of digitally networked spaces, services, and technologies that children access and interact with.
- **digital platforms**: Online services or applications where users interact, such as social media, messaging apps, and websites.
- **digital tools**: Software or applications used to facilitate tasks or communication online.
- **technology-enabled systems**: Systems that use digital technologies to deliver services, such as child helplines or support portals.

Partners

In partnership with:

Office of the Director
International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435

Office of the Deputy Director
Operations Coordination Department (DDR)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5131

Digital Networks and Environment Department (DNE)
Email: bdt-dne@itu.int
Tel.: +41 22 730 5421

Digital Knowledge Society Department (DKS)
Email: bdt-dks@itu.int
Tel.: +41 22 730 5900

Projects, Partnerships and Digital Skills Department (PPS)
Email: bdt-pps@itu.int
Tel.: +41 22 730 5447

Africa

Ethiopia

International Telecommunication Union (ITU) Regional Office
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopia

Email: itu-ro-africa@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroon

Union internationale des télécommunications (UIT)
Bureau de zone
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Cameroon

Email: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

Senegal

Union internationale des télécommunications (UIT)
Bureau de zone
8, Route du Méridien Président
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar - Yoff
Senegal

Email: itu-dakar@itu.int
Tel.: +221 33 859 7010
Tel.: +221 33 859 7021
Fax: +221 33 868 6386

Zimbabwe

International Telecommunication Union (ITU) Area Office
USAF POTRAZ Building
877 Endeavour Crescent
Mount Pleasant Business Park
Harare
Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 242 369015
Tel.: +263 242 369016

Americas

Brazil

União Internacional de Telecomunicações (UIT)
Escritório Regional
SAUS Quadra 6 Ed. Luis Eduardo Magalhães,
Bloco "E", 10º andar, Ala Sul (Anatel)
CEP 70070-940 Brasilia - DF
Brazil

Email: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados

International Telecommunication Union (ITU) Area Office
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados

Email: itubridgetown@itu.int
Tel.: +1 246 431 0343
Fax: +1 246 437 7403

Chile

Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Santiago de Chile
Chile

Email: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras

Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras

Email: itutegucigalpa@itu.int
Tel.: +504 2235 5470
Fax: +504 2235 5471

Arab States

Egypt

International Telecommunication Union (ITU) Regional Office
Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypt

Email: itu-ro-arabstates@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia-Pacific

Thailand

International Telecommunication Union (ITU) Regional Office
4th floor NBTC Region 1 Building
101 Chaengwattana Road
Laksi,
Bangkok 10210,
Thailand

Email: itu-ro-asiapacific@itu.int
Tel.: +66 2 574 9326 – 8
+66 2 575 0055

Indonesia

International Telecommunication Union (ITU) Area Office
Gedung Sapta Pesona
13th floor
Jl. Merdeka Barat No. 17
Jakarta 10110
Indonesia

Email: bdt-ao-jakarta@itu.int
Tel.: +62 21 380 2322

India

International Telecommunication Union (ITU) Area Office and Innovation Centre
C-DOT Campus
Mandi Road
Chhatarpur, Mehrauli
New Delhi 110030
India

Email:
Area Office: itu-ao-southasia@itu.int
Innovation Centre: itu-ic-southasia@itu.int
Website: ITU Innovation Centre in New Delhi, India

CIS

Russian Federation

International Telecommunication Union (ITU) Regional Office
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation
Email: itu-ro-cis@itu.int
Tel.: +7 495 926 6070

Europe

Switzerland

International Telecommunication Union (ITU) Office for Europe
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: eurregion@itu.int
Tel.: +41 22 730 5467

International Telecommunication Union
Telecommunication Development Bureau
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN 978-92-61-41731-4

9 789261 417314

Published in Switzerland
Geneva, 2025