FUNDING SAFE DIGITAL FUTURES FOR CHILDREN: A PUBLIC FINANCE ROADMAP FOR CHILD SAFETY IN DIGITAL SPACES

STRATEGIC BRIEF



Partners

Safe Online · brave movement · 5RIGHTS FOUNDATION · ChildFund International · CHILDLIGHT · ECPAT · IWF Internet Watch Foundation · toto NEWS · PLAN INTERNATIONAL · World Vision

This is a joint effort of the Safe Digital Futures – Invest in Children Coalition under the leadership of World Vision International and with financial contributions from Safe Online, World Vision International, Childlight - Global Child Safety Institute and ChildFund International.

CITATION SUGGESTION
Cornerstone Economic Research (2026). Strategic Brief: Funding Safe Digital Futures for Children. Commissioned by the Safe Digital Futures – Invest in Children Coalition.

CONTACT PERSON
Tamara Tutnjevic Gorman
Senior Director, Policy and Influencing (Global)
World Vision International
email: tamara_tutnjevic@wvi.org

PROJECT TEAM
Conrad Barberton
conrad@cornerstonesa.net
Senior Economist with Cornerstone Economic Research

Jonathan Carter
jonathan@cornerstonesa.net
Senior Economist with Cornerstone Economic Research

Gwen Dereymaeker
g.dereymaeker@gmail.com
Senior Research Associate

Carmen Abdoll
carmen@cornerstonesa.net
Economist with Cornerstone Economic Research

Table of Contents

1 THE INVESTMENT MANDATE FOR CHILD SAFETY IN DIGITAL SPACES 5

2 CORE POLICY PRINCIPLES: REFRAMING HOW DIGITAL SAFETY IS FINANCED 7
2.1 GENERAL TAX REVENUE IS THE CORE BASE 7
2.2 THE POLLUTER PAYS PRINCIPLE GOVERNS TECHNOLOGY OVERSIGHT 7
2.3 PREVENTION YIELDS THE HIGHEST SOCIAL AND FISCAL RETURN 8
2.4 HAVE REALISTIC EXPECTATIONS FOR INNOVATIVE FINANCE 8
2.5 PLACE STRICT LIMITS ON STATE BORROWING 8
2.6 ETHICAL BOUNDARIES AND PUBLIC FINANCE INTEGRITY 8
2.7 INSTITUTIONAL CAPACITY AND INDEPENDENT DATA DRIVE INVESTMENT 8

3 THE THREE-LAYER SYSTEMS ARCHITECTURE 9
3.1 LAYER 1: COORDINATED INTERNATIONAL ARCHITECTURE (PHASE 2 HORIZON) 9
3.2 LAYER 2: NATIONAL SYSTEM ENABLEMENT 10
3.3 LAYER 3: THE CONTINUUM OF CARE 11

4 THE PLANNING, COSTING, AND FUNDING CYCLE 12
4.1 PHASE I: PLAN (STEPS 1 TO 3) 12
4.2 PHASE II: COST (STEP 4) 12
4.3 PHASE III: FUND (STEPS 5 AND 6) 13

5 FUNDING PATHWAYS FOR CHILD SAFETY IN DIGITAL SPACES 14

6 SEQUENCING AND DEPENDENCIES: WHAT MUST BE FUNDED FIRST 16

7 STRATEGIC ADVOCACY AND MULTI-STAKEHOLDER DECISION-MAKING 17
7.1 MANAGING TECHNOLOGY INDUSTRY INFLUENCE 17

8 RECOMMENDATIONS AND PRIORITY ACTIONS 19
8.1 RECOMMENDATIONS 19
8.2 PRIORITY ACTIONS FOR THE NEXT 12 MONTHS 21

ANNEXURE 1 FUNDING PATHWAYS: VIABLE TOP-UP SOURCES AND LIC PATHWAYS 22

Key public finance terms used in this brief:

Term	Meaning in this implementation guidance
General tax revenue:	Standard government revenue from income, business, and sales taxes, pooled and distributed through the annual budget.
On-budget spending:	The use of public or philanthropic money to reduce the risk or raise the return for private investors, so that they invest where they otherwise would not.
Recurrent vs. capital costs:	Recurrent refers to ongoing operational costs that continue every year (such as salaries and office rent). Capital refers to physical, long-lasting equipment and buildings.
Supervisory fees:	Mandatory fees paid by regulated technology companies to cover the government's cost of supervising them (it is not a fine, nor a licence to cause harm).
Medium-Term Expenditure Framework (MTEF):	A multi-year rolling budget plan (usually three years) that sets spending ceilings across ministries.



1 The Investment Mandate for Child Safety in Digital Spaces

Governments across the world increasingly agree on what must be done to protect children from technology-facilitated harm. They know that children face escalating threats across digital environments, spanning abusive content, predatory contact, harmful conduct, and exploitative commercial contracts. Yet, despite widespread political commitment, governments face a severe implementation barrier: they agree far less on how to pay for the required solutions.

For more than a decade, efforts to protect children online have relied heavily on fragmented, short-term project grants, philanthropic donations, and voluntary initiatives by technology companies. This model does not work. Online harms are surging, as demonstrated by the seven-fold growth in the number of suspected child sexual exploitation reports recorded in jurisdictions like the Philippines between 2019 and 2021 (from 400,000 to over 2.8 million). In addition, traditional external finance is shrinking rapidly: official development assistance (ODA) from OECD Development Assistance Committee members fell by 23.1% in 2025 alone.

This Strategic Brief aims to provide a clear, practical public finance roadmap for decision-makers – particularly Ministers of Finance, Planning, ICT, and Child Protection. It translates the findings of the 2026 Global Implementation Guidance into actionable policy directions. The central message of this brief is that child safety in digital spaces requires a permanent, institutionalised public system. To build and sustain this system, governments must shift from ad-hoc project-based funding to structural public funding.

Key messages

1. **General tax revenue should fund most of the system.** Domestic tax revenue is the primary and most sustainable source of funding and should fund the core recurrent costs of the system, especially salaries.
2. **Supervisory fees, which cover the cost of supervising the technology industry, should fund the regulator.** A permanent share of the regulator's budget should come from general tax revenue, so that oversight continues if fee income falls or is challenged in court.
3. **The technology industry should pay for its own compliance.** The law should set what companies must do, and companies should bear the cost of doing so. They should make no direct payments to the bodies that oversee or investigate them.
4. **Donor funds should cover set-up costs.** Grants and technical assistance can fund establishment and one-off costs. Recurrent costs should be funded from the national budget from the outset.
5. **Borrowing should be used only for lasting capital assets.** The public functions of this system generate no revenue from which debt could be repaid , **and** therefore borrowing is justified only for assets that last.
6. **Start with a lead ministry, a costing and a budget allocation.** Services cannot be funded predictably until the system has an owner with the authority to convene other ministries and lead the development of the system.

7. **Build the national system as well as the services.** Laws, a regulator, coordination, a trained workforce and independent data are essential for the delivery of services and must be resourced.
8. **Prioritise prevention.** Intervening early, and requiring platforms to remove hazards at the design stage, protects more children at lower long-term cost than relying only on law enforcement and on recovery services after harm has occurred.
9. **Fund cross-border functions together.** Shared databases, standards and cooperation benefit all countries. In Phase 1, countries should build on existing institutions and initiatives, funded through voluntary multi-year contributions tiered by fiscal capacity. In Phase 2, these functions could be brought together in a standard-setting International Agency and an International Solidarity Fund. This brief treats these as a direction of travel, not a design proposal.
10. **Do not rely on innovative finance for core funding and never put a price on harm.** The system that is needed does not generate funds that could be used to repay investors.

Building on the investment-case work on ending violence against children

This brief reflects the planning and costing approach described in *Building the investment case for ending violence against children: Toolkit* published by the Office of the Special Representative of the Secretary-General on Violence against Children in 2025, and subsequently applied in the three investment-case briefs prepared for UNICEF for the second Global Ministerial Conference on Ending Violence against Children, to be held in Manila (Philippines) in November 2026:

- Brief 1 – Supporting parents and caregivers, protecting children: the investment case for universal parent and caregiver support.
- Brief 2 – Making schools safe and enabling: the investment case for safe and enabling school environments.
- Brief 3 – Child protection systems, a critical investment for prevention and response: the investment case for strengthening child protection systems.

Each UNICEF brief addresses one of the three breakthrough approaches of the 2024 Bogotá Call to Action and sets out the process for developing an inputs-based costing tool, which can be used as an implementation plan and inform budget submissions.

2 Core Policy Principles: Reframing How Digital Safety is Financed

To establish sustainable financing, economic and social policy must be guided by the following foundational principles grounded in public finance realities and empirical lessons from the health, education, and climate sectors:

2.1 General tax revenue is the core base

Domestic tax revenue is the single most predictable, equitable, and sustainable source of finance for public systems. Funding must be integrated within existing sector budget votes (education, health, police, social welfare) and increased to cover recurrent operational costs, especially the salaries of child protection workers, teachers, prosecutors, and specialist investigators. Standalone online safety projects funded by external aid create fragile funding dependencies that collapse once donor cycles end.

2.2 The polluter pays principle governs technology oversight

Making products and services safe is the legal and commercial responsibility of the technology providers that profit from them. Regulated companies must pay statutory supervisory fees to cover the state's cost of oversight. Paying these fees or fines is not a licence to cause harm or a waiver of legal duties.

The methods for calculating the fees must be set in primary legislation so that they withstand judicial challenges. Revenues generated by these fees should go into national revenue funds and be allocated to the regulatory authority through the annual national budget approved by parliament.



2.3 Prevention yields the highest social and fiscal return

A public health approach organises interventions into three categories:

- Primary – stopping harm before it occurs,
- Secondary – early intervention for vulnerable groups, and
- Tertiary – reactive response and recovery.

Tertiary interventions are essential but expensive, resource-intensive, and often exact an emotional toll on providers. Universal safety-by-design and school-based prevention reach all children and reduce long-term fiscal burdens across health and justice systems.

2.4 Have realistic expectations for innovative finance

Novel financial mechanisms (such as blended finance, impact bonds, or private equity vehicles) cannot substitute for public funds. Blended finance mobilises private capital weakly in social sectors: evaluations reveal that each public dollar invested in developing countries mobilises only $0.75 of private capital – and merely $0.37 in low-income countries (LICs)[1]. Child safety functions generate no commercial revenue streams from which private capital can be repaid.

2.5 Place strict limits on state borrowing

Sovereign borrowing must never fund recurrent operational expenses or regulatory administration. Concessional borrowing is justified only as a last resort for long-life physical capital, such as specialised digital forensic laboratories. Child safety requirements should instead be integrated as non-negotiable standards within large-scale digital public infrastructure and connectivity loans already financed by multilateral development banks and bilateral lenders. To account for varying creditor conditionalities and transparency standards, borrowing governments must embed these safeguards upstream during project design and technical procurement specifications, ensuring they bind all infrastructure investments regardless of the financing partner.

2.6 Ethical boundaries and public finance integrity

Market-based mechanisms that price, trade, or permit harm are fundamentally rejected; this rules out sin taxes or tradable allowances on abuse. Similarly, outcome-based financing and impact bonds are explicitly excluded. In child safety, proving that a specific programme caused a reduction in hidden harm is virtually impossible, and tying investor returns to children's welfare carries unacceptable ethical risks.

2.7 Institutional capacity and independent data drive investment

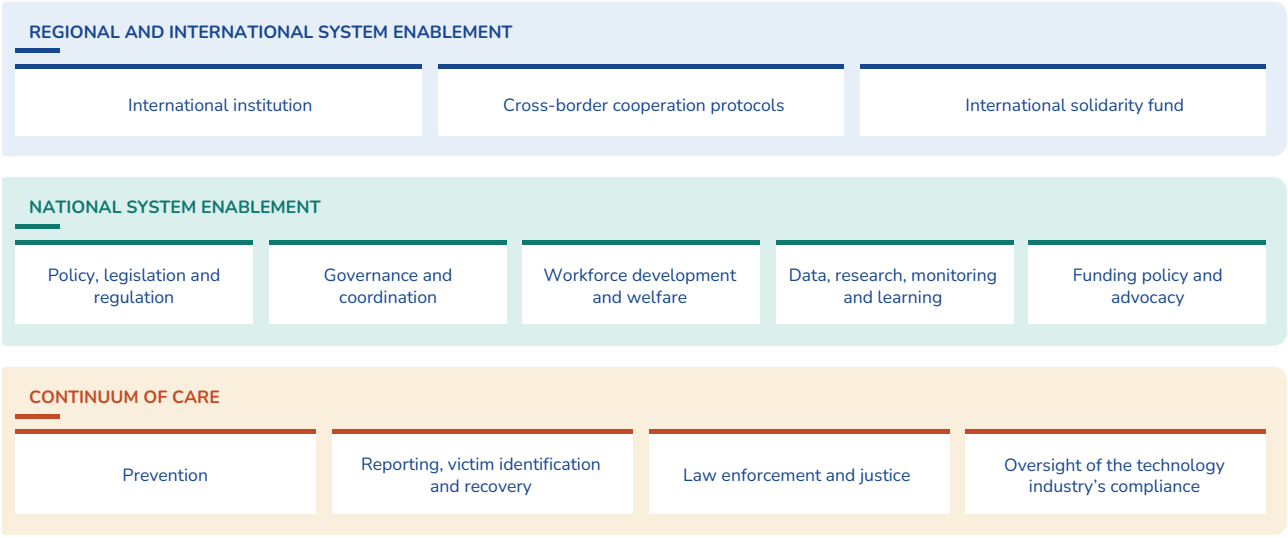
Systems fail from **a lack** of administrative and technical capacity far more often than from raw capital shortages. Governments must invest early in independent data systems, establishing national baseline surveys and performance metrics rather than relying on self-serving corporate transparency reports.

[1] https://odi.org/en/publications/blended-finance-in-the-poorest-countries-the-need-for-a-better-approach/

3 The Three-Layer Systems Architecture

Ensuring child safety in digital spaces requires an interconnected public system organised across three operational layers (Figure 1). These layers link global standards and cross-border cooperation down through national laws to the daily frontline services that protect children in schools, communities, and health clinics:

Figure 1 The Layers of the Systems Architecture for Child Online Safety



The layers operate as an interdependent system:

- The effectiveness of the international standards and shared databases depends on national governments passing enforceable laws and designating responsive central authorities to act on cross-border evidence.
- National laws, coordination mechanisms, and trained staff provide the administrative foundations for the frontline clinics, schools, police units, and helplines.
- Frontline disclosures and case volumes supply the empirical data that refines national policy, adjusts multi-year budget requests, and informs international safety-by-design standards.

2.1 Layer 1: Coordinated International Architecture (Phase 2 Horizon)

Online harms routinely cross borders: a single case can involve a child, an offender, a hosting provider, and a payment processor based in four different countries. Because no country can tackle digital harms alone, shared international infrastructure is needed to provide vital global public goods. Rather than creating an expensive new bureaucracy immediately, the implementation guidance proposes a two-phase approach:

- **Phase 1 (Immediate Horizon):** Countries coordinate through existing multilateral bodies and operational networks. Shared technical infrastructure, such as INTERPOL's International Child Sexual Exploitation (ICSE) database and the INHOPE global network of reporting

hotlines, continues to anchor victim identification and cross-border content removal. Policy coordination, research alignment, and catalytic grant funding build directly on the Safe Online fund, the WeProtect Global Alliance, the Global Online Safety Regulators Network, and state-led initiatives such as the Coalition for Children's Rights and Protection in the Age of AI. Member states support these functions through voluntary multi-year contributions.

- **Phase 2 (Medium-Term Horizon):** Over the medium term, governments could consider bringing these functions together in a more formal international architecture to unify global standards and long-term financing. This brief treats the elements below as a direction of travel, not a design proposal; their form, hosting and financing are for governments to decide:
- **An International Agency:** Provisionally named the International Agency for Child Safety in Digital Spaces, which could be established as a new body or hosted as an incremental mandate within an existing multilateral organisation to share overheads and minimise costs. Such an agency could set global standards for technology provider conduct (such as mandatory safety-by-design, automated abuse detection, and algorithmic audits), develop model national laws, and publish independent audits of platform compliance.
- **Cross-Border Cooperation Protocols:** Could standardise mutual legal assistance, rapid electronic evidence preservation, cross-border content takedowns, and victim support through designated national central authorities, operationalising mutual legal assistance treaties and the UN Convention against Cybercrime.
- **An International Solidarity Fund:** A pooled multilateral financing facility that could have two separate windows: an Institutional Window (covering the core operating budget of the International Agency and protocol secretariat, possibly funded by assessed member-state contributions linked to ability to pay) and a Capacity Window (pooling development assistance and philanthropic grants to fund initial technical setup, national central authorities in lower-income countries, and shared regional forensic hubs).

3.2 Layer 2: National System Enablement

National system enablement provides the legislative, institutional, and technical foundation that makes service delivery possible and sustainable. It consists of the following components:

- **Policy, legislation, and regulation:** Enacts primary child digital safety legislation, defines procedural rules for digital evidence, establishes legally binding duties of care on technology providers (mandating safety-by-design and rapid content takedown), creates an independent online safety regulator, and embeds child protection requirements into the design of national digital public infrastructure and connectivity.
- **Governance and coordination:** Designates a single national lead ministry with the statutory authority to convene across sectors (education, health, social welfare, police, and justice). It formulates a multi-year national strategy, coordinates implementation, and institutes permanent, budgeted mechanisms for child and survivor consultation.
- **Workforce development and welfare:** Embeds digital safety competencies into existing training **curricula** for teachers, social workers, healthcare staff, police, and prosecutors. Crucially, it recognises the need to provide mandatory, institutionalised mental health support and vicarious trauma counselling for frontline personnel and analysts exposed to graphic abuse material, funded as a standing operational cost to prevent workforce burnout and turnover.

- **Data, research, monitoring, and learning:** Funds regular national prevalence surveys, establishes routine administrative reporting across police and social services, and supports independent monitoring by academic bodies and civil society, ensuring policy and budgets are driven by verified evidence rather than self-reported corporate transparency metrics.
- **Funding policy and advocacy:** Equips finance and planning ministries to cost national systems from the ground up, structure enforceable supervisory fees on the technology sector, and protect dedicated allocations for child digital safety within annual budgets and MTEFs.

3.3 Layer 3: The Continuum of Care

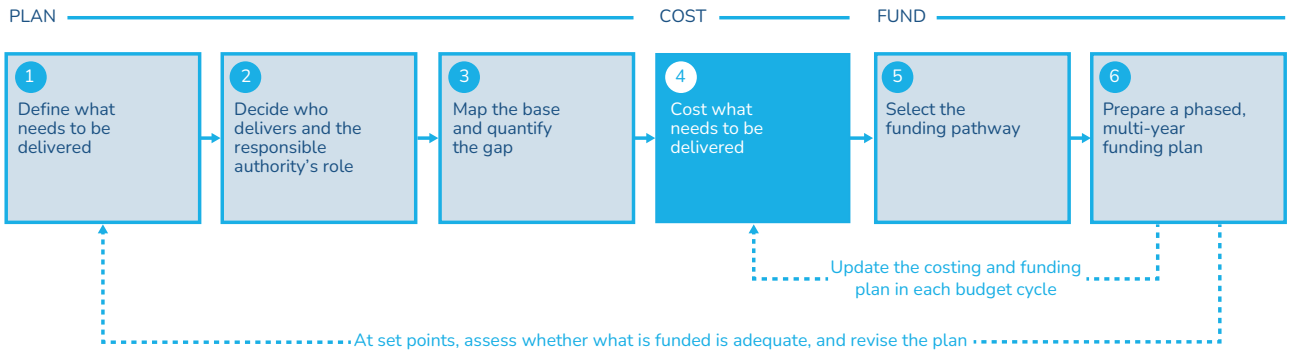
The Continuum of Care represents frontline service delivery where public systems interact directly with children, caregivers, and communities. Most of these services are delivered through existing public infrastructure in health, education, social welfare, policing, and justice; technology-facilitated harm adds new cases rather than requiring separate frontline institutions. It spans the following service components:

- **Prevention services:** Delivers evidence-based online safety education integrated into national school curricula (such as the Safe to Learn framework), universal parenting support programmes that help caregivers guide children's digital use, targeted community awareness, and specialised interventions for individuals at risk of committing offences.
- **Reporting, victim identification, and recovery:** Operates free, 24/7 child helplines (phone and online chat), national reporting hotlines affiliated with INHOPE, specialised victim identification units linked to INTERPOL's ICSE database, statutory notice-and-takedown procedures, and long-term medical, psychological, and trauma recovery care.
- **Law enforcement and justice:** Maintains dedicated police cybercrime investigation units, modern computer forensic laboratories, specialised prosecution teams, child-friendly court procedures, legal aid, and victim compensation funds. Because forensic technology becomes obsolete quickly, procurement must include a budgeted lifecycle replacement fund from the outset, so equipment can be regularly upgraded.
- **Oversight of technology industry compliance:** Covers the work of the independent regulator: conducts regular audits, algorithmic risk assessments, platform inspections, and investigations of non-compliance, backed by the power to issue binding improvement notices and administrative financial penalties.

4 The Planning, Costing, and Funding Cycle

Governments must follow a disciplined, inputs-based public financial management cycle across all layers to turn policy ambition into funded budgets (Figure 2). Systems must be **planned**, costed and made fit for context.

Figure 2 Planning, Costing, and Funding Cycle



4.1 Phase I: Plan (Steps 1 to 3)

Step 1: Define what needs to be delivered. Break each system component down into concrete operational functions, defining measurable quality and coverage standards, for example, maximum response times for helpline calls, forensic examination turnaround standards, maximum hours for illegal content takedown, and school curriculum content.

Step 2: Decide who delivers and the authority's role. Governments determine the delivery mechanisms, which can include direct state provision, agreements with state-commissioned non-governmental organisations (frequently used for child helplines and reporting hotlines), or statutory corporate duties placed on private firms. The tasks that are the legal duty of technology companies, such as automated abuse detection, content removal, age verification, and risk mitigation, must be delivered and financed directly by the companies themselves.

Step 3: Map the base and quantify the gap. Ministries must conduct rigorous mapping of existing legislation, institutional capacities, public expenditures, and external donor flows. This includes identifying spending already embedded in programmes funded through ICT, education, and policing budgets. This is essential to calculate the incremental gap, preventing double-counting and showing ministries of finance what extra resources are genuinely required.

4.2 Phase II: Cost (Step 4)

Step 4: Involves translating operational plans into cost estimates using an inputs-based costing approach guided by the core formula *Cost = Quantity × Input × Price*, in which the inputs that are needed are quantified and local unit prices are used to estimate costs. The costing process must distinguish between:



- **One-off and recurrent costs:** The cost of one-off activities needed to establish the system, such as drafting legislation, setting up regulatory technology and designing initial training curricula, must be costed separately from recurrent costs, such as salaries, operational overheads and annual system licences, that are needed to maintain the system.
- **Existing vs new costs:** Some activities can be absorbed into existing budgets at little extra cost (like adding digital safety into regular teacher training), while new services require additional funding.
- **Planning for rising demand:** As awareness campaigns succeed, helpline calls and police reports are likely to increase. Budgets must plan for higher caseloads, though the cost per case should drop as operations scale up.

Unit costs should not be borrowed from other countries, as differing wage scales, population densities, and operating models make imported values misleading.

4.3 Phase III: Fund (Steps 5 and 6)

Step 5: Select the matching funding pathway. The funding mechanisms used must fit what is funded. Additional allocations for salaries and other recurrent costs should be funded from core government budgets, which are usually funded from domestic tax revenues. Some regulatory functions can be funded from levies, and borrowing could be considered for the few items of capital expenditure that may be needed.

Step 6: Prepare a phased multi-year funding plan. The relevant costing results are transferred into budget submissions so that these meet the requirements of budget circulars, both in terms of timing and depth of detail. The phased multi-year plan must be aligned with the pace at which institutions can develop and absorb additional capacity.

5 Funding Pathways for Child Safety in Digital Spaces

Sound public finance practice holds that the funding of a system for ensuring child safety in digital spaces should consider the following:

- **Fund core operations from the national budget:** Placing core operational staff directly on the national public payroll safeguards institutional knowledge and provides the staffing stability these services need to function. Using donor grants and technical assistance strictly for one-off setup costs, such as drafting legislation, rolling out IT platforms, and designing training courses, ensures essential public services continue running smoothly without facing sudden funding cliffs when external projects end.
- **Budget for the full lifecycle of capital purchases:** Budgeting for multi-year maintenance and scheduled hardware replacements alongside every major technology purchase keeps high-tech forensic labs fully operational and up to date, allowing cases to keep moving without interruption.
- **Legislate industry levies alongside a core budget allocation:** Setting out clear industry supervisory fees in primary law gives the regulator a reliable, self-funding revenue stream. Backing this with a steady baseline allocation from general tax revenue ensures oversight work, staffing, and enforcement carry on without disruption, even during periods when fee income may be constrained due to legal challenges or sector downturns.

Sustainable service delivery across the child digital safety architecture needs to rest on three fiscal pillars: domestic general tax revenues, statutory industry supervisory fees, and targeted international pooling structures. How these should be used across the system layers to guarantee predictable funding for setup, operational maintenance, and long-term capital replacement is summarised below. Viable top-up sources and LIC pathways for each component are shown in Annexure 1.

System component	Capital and Set-Up Costs (One-Off)	Recurrent Operations and Salaries	Commercial Technology Sector Obligation
LAYER 1: COORDINATED INTERNATIONAL ARCHITECTURE			
1. International Agency			
Phase 1	Multilateral seed grants and project preparation funds	Voluntary multi-year member state contributions (tiered by fiscal capacity)	None (consultative Industry Reference Group; zero governance)
Phase 2		To be decided; options include assessed member-state contributions	None
2. Cross-border cooperation protocols	Technical assistance to design standard operating procedures	Domestic police and justice budgets (dedicated annual budget for the national cross-border liaison office)	Statutory cooperation, secure direct digital connections for lawful police data requests.
3. International Solidarity Fund			

System component	Capital and Set-Up Costs (One-Off)	Recurrent Operations and Salaries	Commercial Technology Sector Obligation
Capacity Window	Donor and philanthropic pooling (catalytic seed grants; Safe Online) for LICs		None (voluntary arm's-length contributions strictly uncapped/ ungoverned)
Institutional Window		To be decided; options include multi-year member contributions and long-term digital levies	
LAYER 2: NATIONAL SYSTEM ENABLEMENT			
4. Policy, legislation and regulation	Bilateral grants and technical assistance for legal drafting	Domestic general tax revenue transitioning to statutory supervisory fees	Mandatory compliance with statutory duty of care and safety-by-design
5. Governance and coordination	Technical assistance for strategy design and costing models	Domestic general tax revenue (lead ministry programme budget line)	Mandatory participation in structured consultative hearings
6. Workforce development and welfare	Donor grants for initial specialist curricula and master trainers	Absorbed within sector personnel budgets (education, police, health)	None (public service capacity and standing trauma support)
7. Data, research, monitoring and learning	Co-financing and trust funds for baseline survey methodologies	National statistics office budget and line ministry monitoring allocations	Mandatory provision of compliance, risk, and algorithmic audit data
8. Funding policy and advocacy	Technical assistance for inputs-based costing and fiscal modelling	Ministries of finance and planning operating budgets; arm's-length NGO grants	None (independent public oversight and expenditure tracking)
LAYER 3: THE CONTINUUM OF CARE (FRONTLINE SERVICES)			
9. Prevention services (schools and community)	Grants for curriculum design, digital modules and campaign assets	Domestic education and social welfare budgets (absorbed at 85%+)	Deploy safety-by-design, parental tools and deterrence alerts at own expense
10. Reporting, victim identification and recovery	IT setup grants, hotline software and INTERPOL ICSE links	General tax revenue; national telecom development funds (routine fees collected from phone and internet operators)	Mandatory 24-hr takedown duty and automated hash-matching at own cost
11. Law enforcement and justice	Grants and concessional debt (assets only: forensic hardware)	National police and justice votes + budgeted lifecycle replacement reserve	Preservation of electronic evidence and 24/7 dedicated law enforcement liaison
12. Oversight of technology industry compliance	Technical assistance for digital audit and algorithmic tools	Statutory supervisory fees levied on platforms backed by a permanent residual share of general tax revenue	100% of supervisory fees and full cost of regulatory compliance audits

6 Sequencing and Dependencies: What Must Be Funded First

Public funding delivers results most cost-effectively when investments are sequenced correctly. Funding public awareness campaigns before survivor support services are in place overwhelms frontline clinics and social workers. Safety regulations cannot be enforced without an empowered regulator. Policy interventions must build the legal and operational foundations before scaling public demand.

The table below lists and substantiates the order of key investments.

What Must Be Funded First	Why this Order Matters
1. Lead ministry, costing and budget programmes	Puts an identifiable minister in charge, ensuring local community services get steady funding year after year instead of running out of money between short-term grants.
2. Statutory duty and regulatory mandate	Empowers the regulator with binding enforcement teeth and independent revenue-collection powers, guaranteeing industry compliance and self-sustaining market oversight.
3. Common standards for the technology industry's conduct	Standards take effect only when national regulators can enforce them. In Phase 1, they can draw on existing frameworks.
4. National legal bases and central authorities	Cross-border protocols depend on each country designating and funding a central authority.
5. Connection to shared databases	Victim identification and hotlines gain most of their value from connection to international databases and networks. These databases and networks already exist and can be used from Phase 1.
6. A trained and supported workforce	Helplines, investigations and prevention depend on staff trained and supported through the national enablement layer.
7. Data, evaluation and learning	Coverage targets, costings and standards are updated as evidence accumulates.

7 Strategic Advocacy and Multi-Stakeholder Decision-Making

Getting funding into budgets requires convincing those who hold the purse strings that the investment is worthwhile and saves public money in the long run. Advocacy for child online safety must move beyond moral appeals and present rigorous, stakeholder-tailored messages to Ministries of Finance, sectoral leaders, and parliamentarians. These are discussed below.

Role players	Messages about the system that may convince them to support its funding and implementation
Ministries of Finance and Treasury	• It prevents downstream costs: Investing in primary prevention avoids massive downstream health and criminal justice expenditures. • The industry will cover its costs: Regulatory supervision is largely funded via fees, placing only a limited net burden on the fiscus. • Clear budget codes allow ministries to track and report on spending across departments.
Lead and Sector Ministries (Education, Justice, Welfare)	• Digital safety can be integrated into existing service mandates rather than creating competing operational silos. • Teacher and social worker capacities must be strengthened holistically. • Staff welfare budgets protect specialised personnel from burnout and turnover.
Parliaments and Legislative Committees	• The system establishes robust statutory accountability over multinational technology platforms. • Legislated fees and levies ensure the regulator is largely self-funded. • Independent prevalence data enables rigorous parliamentary oversight.
Multilateral Development Banks	• Concessional technical assistance is a viable way to fund national system costing and regulatory capacity. • Mandatory child-safety covenants can be embedded in digital infrastructure loans.
Contributing Donors and Philanthropies	• Supporting the International Agency creates global public goods. • Capacity Window financing enables low-income nations to transition to domestic financing.

7.1 Managing Technology Industry Influence

Commercial technology providers are indispensable technical actors, but public authorities must maintain rigorous boundaries to safeguard regulatory independence. The following broad principles apply:

- **Strict firewall between compliance and regulatory governance:** Technology companies must have no voting seats, veto power, or direct sponsorship roles over enforcement agencies, hotlines, or governing boards.

- **Consultative dialogue only:** Technology sector dialogue should occur exclusively through a structured, consultative Industry Reference Group that shares emerging technical threats and safety innovations without participating in regulatory enforcement or funding decisions.
- **No direct corporate payments to law enforcement:** Technology companies must never directly fund police units, prosecutors, or regulators. All company contributions must be paid as mandatory statutory fees or levies to the national treasury to protect regulatory independence.
- **Innovative finance cannot substitute for national tax funding:** When considering financing options, governments must ask: Who repays and from what? Can results be tracked without compromising child privacy? Does the mechanism reduce the technology sector's obligation to obey the law?



8 Recommendations and Priority Actions

8.1 Recommendations

The recommendations below are addressed to the people who can act on them. Much of the planning can be done within a year. The first steps do not need to wait for a costing or an investment case.

Governments should

- Name a lead ministry that has the authority to bring other ministries together, own the strategy and the costing, and lead annual budget submissions.
- Carry out the situational analysis and budget mapping and start developing a context-specific costing from the ground up that is based on national standards and prices. Include the coordination, regulation, workforce and data functions, and separate one-off from recurrent costs.
- Put funding for child safety in digital spaces into the next MTEF, with a programme or sub-programme in the lead ministry's budget and lines in sector budgets, as appropriate.
- Pass a law that (1) places the duty on technology companies to act in children's best interests, design safe products, remove illegal material quickly, cooperate with the police and share data for research; and (2) gives the regulator the legal mandate to charge fees, with the fee base and method set in the law.
- Fund the child safety part of services inside existing education, health, social welfare, police and justice programmes; check helpline and hotline budgets against call volumes every year; and fund psychosocial support for children and for staff as standing costs.
- Name and fund a central authority for cross-border cooperation; connect to INTERPOL's database and the INHOPE network if not yet done; sign and ratify the UN Convention against Cybercrime.
- Embed child-safety requirements into large-scale digital connectivity and public infrastructure at the project design phase, and ensure this is reinforced by conditions on any loans to such projects before procurement begins and contracts and loans are finalised.

Ministries of finance should

- Support the restructuring of budgets of relevant ministries to ensure funding is allocated to where it is needed and can be traced.
- Use supervisory fees to recover the cost of regulation from the industry, while keeping a permanent share of the regulator's budget on general tax revenue.
- Borrow only to finance long-life assets, never to fund running costs.
- Record external support in the budget and agree, from the start, the timetable on which running costs need to be funded from domestic resources.

The Global Ministerial Conference, the G20 and regional bodies should

- Use suitable international forums to signal support for exploring coordinated international financing for child safety in digital spaces as a Phase 2 priority.

- Give technology-facilitated harms more weight in the pledges that follow international forums, including national commitments to name a lead ministry and design and cost the national system.
- Through the AU, ASEAN, the EU and others, host work on model laws, pooled regulatory and audit capacity, regional forensic hubs and specialist training, and keep the agenda moving between conferences.

Development partners, donors, development banks and philanthropy should

- Fund setup and build capacity, but never subsidise what technology companies are legally required to do, nor fund recurrent staff salaries indefinitely.
- Focus grants and technical help on design, set-up, the first groups of trainees and shared regional capability, and channel support through national budgets rather than parallel projects.
- Make child-safety requirements a condition of lending for digital infrastructure, and fund technical help for national gap analyses and costings.
- Fund independent monitoring and independent civil society advocacy at arm's length and over several years.
- Never pay for the safety features, detection tools or moderation staff that the law already requires companies to provide.

The technology industry should

- Build safety into products now, without waiting for international standards, and treat legal duties and supervisory fees as a cost of doing business, recognising that neither one settles the duty to protect children.
- Share expertise through the Industry Reference Group and provide the data the law requires for research and monitoring.
- Refrain from seeking any say over governance or funding of national and international bodies established to regulate the industry.

The Safe Digital Futures – Invest in Children Coalition and civil society should

- Make the case to governments, regional bodies and development banks about the need to direct resources to prevent harms to children in digital spaces, including the case that the costs of doing nothing already land on public budgets.
- Promote credible expectations about innovative finance in policy dialogue, positioning new financial products as a useful supplement to public funding, while keeping the focus on the national and pooled public money the system depends on.
- Bring the voices of children and survivors into this advocacy, in line with the Committee on the Rights of the Child's call for children to be heard on the policy and budget decisions that affect them.

8.2 Priority Actions for the next 12 months

Reforming systems and building new ones takes time, but we cannot afford to wait. The prioritised actions below can be initiated immediately:

Lead Ministry

- Produce a situational analysis and budget mapping and start the costing with the Ministry of Finance.
- Prepare legislation that places a statutory duty on the technology industry and gives the regulator its mandate.
- Work with other governments to map the international institutions, networks and initiatives that already exist, and agree which functions they can take on in the first phase of building the international layer.

Ministry of Finance

- Issue budget guidelines instructing all ministries on how to label and track digital safety spending in their annual submissions.
- Start consultations on a contribution formula for international cooperation that is linked to fiscal capacity.

Regulator

- Where the law is in place, begin supervising the technology industry's compliance.
- Prepare a fee base and methodology to be set in law or regulations.

Sector ministries

- Set service standards.
- Connect police and hotlines to INTERPOL's database and the INHOPE network.
- Secure referral pathways to recovery services.
- Sign or ratify the UN Convention against Cybercrime through the justice ministry.
- Integrate digital safety into school curricula and parent and caregiver support programmes.

Annexure 1 Funding Pathways: Viable Top-Up Sources and LIC Pathways

System Component	Viable Top-Up Sources	Low-Income Country (LIC) Pathway
1. International Agency	Multi-donor trust funds and bilateral donor grants for research.	Voluntary contribution linked to fiscal capacity (small symbolic share); technical assistance for setup.
2. Cross-Border Cooperation Protocols	Capacity Window of the Solidarity Fund for low-income state participation.	Solidarity Fund Capacity Window for central authority setup; domestic budget covers staff from day one.
3. International Solidarity Fund	Multi-donor trust funds; bilateral grants pooling official aid.	Net recipient of the Capacity Window for infrastructure and capital; small voluntary contribution to the Institutional Window.
4. Policy, Legislation and Regulation	Earmarked industry levies; technical assistance for legislative drafting.	Bilateral grants and technical assistance for drafting; core regulator salaries on general budget from day one.
5. Governance and Coordination	Earmarked share of ICT levies; grants for consultative workshops.	Grants for strategy formulation; standing national budget line for ongoing inter-ministerial coordination.
6. Workforce Development and Welfare	Bilateral grants for initial specialist curricula and master trainer cohorts.	Grants can fund master trainers and specialist curricula, but routine staff salaries and trauma counselling must be paid by domestic budgets from day one to avoid sudden service collapse when grants end.
7. Data, Research, Monitoring and Learning	Independent grant pools managed separately from government to ensure unbiased reporting.	Technical assistance for methodology; national survey co-financed with domestic share rising each round.
8. Funding Policy and Advocacy	Technical assistance for fiscal modelling; arm's-length grants for civil society.	Technical assistance for costing models; independent donor grants directly to civil society watchdogs.
9. Prevention Services	Corporate statutory duty for online deterrence; earmarked online levies.	Grants and technical assistance for curriculum design; delivery funded through national education budget.
10. Reporting, Victim Identification and Recovery	Dedicated telecom development funds created from standard telecom operator fees.	Grants for helpline IT and analyst training; staff and therapy on national budget/universal service fund; therapy never donor-reliant.
11. Law Enforcement and Justice	Pooled funds for regional forensic hubs; low-interest loans used strictly to buy specialised forensic lab equipment, backed by an annual maintenance savings fund.	Grants for forensic equipment and initial training; domestic budget for salaries, maintenance, and replacement reserve.
12. Oversight of Technology Industry Compliance	General tax revenue as permanent residual floor to cushion fee volatility.	Supervisory fees remain primary (paid by global technology companies); technical aid for audit capacity.

Safe Digital Futures

Invest in Children



















