Chapter 5

# Practical aspects of creating a hotline

While INHOPE will develop this with you through our Country Assessment Framework as shown in <u>Hotline Timeline</u> <u>Creation</u>, you need to have some understanding of the appropriateness of your country and your organisation for setting-up a hotline.

Overall, this means conducting an analysis of the national legislation, the socio-cultural context, and existing efforts to combat the problem in your country.

Specifically, you will need to:

#### 1. Identify the legal basis – will it be possible to set up a hotline?

Specific professional advice should be sought regarding legislation which bears directly on hotline activities. Depending on the type of organisation behind the proposed hotline, it may be possible to get *pro bono* legal support. NGOs have often benefited from *pro bono* legal advice in this area; however, this may be less available to private sector organisations. It is essential to seek support from local specialists, and expect them to provide clear guidance on issues such as (but not limited to):

- How clearly are the legal parameters of child sexual abuse images defined? Is the existing legislation adequate?
- What are the legal implications of looking at an image of online child sexual abuse content?
- Is a cached image, automatically created when the image is viewed, an offence (i.e., does that constitute 'creating' an image)?
- What exemptions would a hotline/hotline employee need to be able to view potentially illegal content to do their iob?
- Are there issues around data storage (e.g., relating to the URLs, files, reporters ID / IP address)?
- Are there issues around maintaining reporter's anonymity?
- What are the hotline's legal liabilities? What might happen if the hotline got sued?
- Does the hotline need to be a registered entity/charity or equivalent?
- What legal requirements are there in terms of ownership, governance, transparency, and accountability?
- What are the national regulations for data privacy and protection? Which policies does the organisation need to
  process this data? Is there a requirement for a hotline to be managed under the auspices of a national authority?
   (e.g., film and classification board, a media and communications authority etc).

#### 2. Build the 'business case' - is there existing research or data on the issue in your country?

Consider engaging with the ministry responsible for children's welfare and the national Children's Ombudsman (if there is one nationally). Equally, engage with national child protection authorities and organisations who can provide in-depth information on the online child exploitation and abuse, and efforts that have already taken place.

#### 3. Initiate multi-stakeholder dialogue

- Identify and bring together the main stakeholders of a hotline.
- Convene a national roundtable and a working group for follow-up if possible. Once there is consensus on the need to develop a hotline you will have your supporters and it will be easier to progress with the same goal.

#### 4. Organise a learning visit to an experienced hotline in another country

After understanding the national context, the hotline should seek to visit an existing hotline with a similar cultural context and operating to a similar scale as the intended new hotline. Ideally key staff should be given the opportunity to spend time 'shadowing' the working day in an existing hotline. This hotline should have a comparable legislative, cultural, and funding background, and similar levels of efficiency to those which are envisaged for the hotline being set up. In order to benefit from direct experience, it would be helpful to visit a hotline which still employs the staff who were involved in the process of setting up the hotline. Whilst it may be of interest to visit the larger established hotlines, it should be remembered that these hotlines have levels of investment, staffing, technology, and operational procedures that are entirely different in scale to those which will be necessary for a new hotline. Contact INHOPE for most relevant contacts to visit an existing hotline in your region.

#### 5. Define the role and remit of the hotline

The hotline's focus can be wider than receiving reports of online CSAM only. While the focus can be purely on ICT-facilitated sexual exploitation and the sexual abuse of children, some hotlines broaden their remit and offer other reporting possibilities. Some INHOPE hotlines receive reports on other topics depending on their mandate. The hotline in Belgium, Child Focus deals with different types of reports, including online CSAM of course, but also child erotica/inappropriate child-related images, child nudism, child grooming activities, trafficking in children for sexual purposes, sexual exploitation of children in travel and tourism and adult pornography (accessible to children). Another example is the hotline in Coombia *TeProtejo*, which deals with, among other topics, cyber bullying and the sale of tobacco, alcohol and drugs to minors. To find out what each hotline is combatting, click here to read our annual report.

Defining the role and remit of work is important to ensure clarity of messaging. As mentioned above, the hotline can widen its remit as long as it publicises itself clearly. By being precise about the subjects on which they receive reports, a hotline is also more likely to gain the confidence of the public, thereby encouraging them to report. The applying organisation should also clearly outline its planned remit and scope in any collaboration with the relevant partners. This helps to define the nature of the cooperation being requested with each partner, and to make sure it is clear and

contained. However, this does not mean that the hotline service should avoid other types of reporting categories if these are important in responding to the local reality in the country.

The hotline must be seen to be independent but with clear reporting lines to the competent authorities, to ensure transparency and accountability.

## 5.1 Considerations for working with key stakeholders

#### 5.1.1 Government

Government support for the hotline initiative will be critical to its success in several ways, including to:

- Manage potential issues related to navigating or re-defining legislation.
- Provide credibility in the eyes of other key stakeholders and the general public.
- Identify opportunities for government funding.
- Enable law enforcement to give the hotline the required levels of assistance.

It is likely that there will be **two main** governmental departments whose approval and involvement will be required:

- The department with a remit for Information and Communications Technology, such as the Ministry of Information and Technology or Communications. This department may:
  - Already oversee an active online safety programme.
  - Play a valuable role in promoting the hotline to the public as part of its wider safer internet activities.
  - Have responsibility for deciding whether the hotline initiative can operate in a self-regulatory way as opposed
    to a formally regulated/legislated environment.
- 2. The department with a remit for law enforcement, such as the Ministry of Justice. This department will be able to:
  - Assist with legislative issues, such as defining the assessment of legal and illegal content.
  - Endorse and oversee involvement by law enforcement with the hotline's work.
  - Authorise and sign a written agreement with the organisation operating the hotline unless the agreement can
    be made directly with law enforcement. This agreement should cover the authorisation of the hotline
    employees to receive, open and assess content, and could be supported by formal approval of the hotline's
    operational procedures regarding the management of illegal content.

As described in the <u>Hotline Creation Timeline</u>, you should always contact law enforcement first, and in parallel, also the relevant governmental department to avoid complications. Each has an important role to play in supporting the hotline, and this needs to be defined early on, for example at the national roundtable or stakeholder meeting.

In some cases, this process may be reversed since these same stakeholders may be involved in selecting and endorsing the organisation that will operate the hotline.

#### 5.1.2 Advisory Board

We also suggest creating an Advisory Board. The members of this council are members who embrace the same cause of protecting the rights of the child, such as non-profit organisations, ministry of justice members, internet service providers, lawyers and other bodies that seek to raise awareness on the cause.

#### 5.1.3 Data Protection Agency

The relevant LEA and hotline organisation will need to collaborate from an early stage with the national data protection agency to understand any implications for the hotline, and its proposed activities and processes. It is imperative that the data processing policies and privacy policies of the hotline are clearly visible on the hotline's website. Each hotline is responsible for its own data protection and the transparent processing of any personal data of reporters.

#### **5.1.4 Law Enforcement Agency**

A strong working relationship with the national law enforcement agency, right from the development stages, will simplify and strengthen the processes relating to the foundation and running of the hotline.

#### Tips for engaging with the national law enforcement agency:

#### Get law enforcement involved early on

Depending on the specific situation in the country, online child sexual abuse material may not be a priority issue for the national LEA. If this is the case, law enforcement will need to be sensitised to the scale of the problem, the wider international backdrop, and the role of a national hotline within this context. Reference can be made to the WEPROTECT Global Alliance Model National Response and to multi-stakeholder cooperation to support local capacity building by the relevant international partners. As such, international law enforcement agencies will play a crucial role not only in sensitising their colleagues to the challenges of online child sexual exploitation and abuse, but also in providing training, evidence of the problem in the country, and operational support. Early involvement of law enforcement helps to avoid a situation where government has become engaged, and the hotline is 'forced' upon law enforcement without warning. This could understandably create resistance, and, in

fact, a later engagement could also fail to fully exploit valuable expertise and consultative support from the LEA during the development stages.

#### Identify the relevant law enforcement unit

In most countries, there is a unit for crimes against children that might also cover issues relating to domestic violence, sexual assault, family crimes and similar. However, this unit may not have a mandate for the 'cyber' dimension of these crimes, and there may be a cybercrime unit that would be expected to lead on these. In countries without a dedicated unit for online crimes against children, this challenge is common – is it a 'cybercrime' to be handled by the cybercrime unit, or a 'real' crime with 'cyber evidence' that should be handled by the child unit?

Because of this, it may be difficult to identify one single unit responsible for investigating online child sexual exploitation. If it is unclear from an external perspective, the relevant government department should be able to define responsibility. As a country develops and implements a national action plan to protect children from online exploitation and abuse, the establishment of a dedicated unit would normally take place. However, in the early stages, a hotline could be required to work with several law enforcement departments.

#### Engage law enforcement at the most senior level

Support and traction for the hotline 'from the top down' is very important. Depending on the organisation(s) involved in setting up the hotline, it can be difficult to get access to a senior figure in law enforcement. If this is the case, INTERPOL, which covers online Child Sexual Exploitation and Abuse through its Vulnerable Communities Sub-Directorate<sup>6</sup>, may be able to assist with an introduction through the country's National Central Bureau (NCB). The Heads of NCBs are typically high up in the national police structure. In addition, the NCBs are the gateway for gaining access to INTERPOL's 'blocking list' named as INTERPOL's International Worst of List. This list consists of domains that contain the most severe child sexual abuse images, which will be of relevance to industry partners seeking to introduce this type of blocking.

Preparation and documentation of the business case will help law enforcement to understand the project and its role in relation to it. The organisation planning to set up the hotline should prepare to present:

- ✓ Information on context, scope, and ambitions for the hotline.
- ✓ Draft proposals for law enforcement's role in the development process.

<sup>&</sup>lt;sup>6</sup> For more information on Vulnerable Communities Sub-Directorate, click here.

✓ Documented and transparent procedures relating to issues such as office and IT security, staff welfare and report processing. These should be clear, but it is important for law enforcement to be invited to help build on them further once there are more involved in the process.

An initial meeting could take place at the premises of the organisation that will operate the hotline, giving law enforcement the chance to see the organisation and visualise operations for themselves. In terms of the ongoing relationship with law enforcement, certain parameters will need to be established, such as:

- ✓ The Memorandum of Understanding, an official agreement.
- ✓ What are the priorities?
- ✓ How much support are they able to provide?
- ✓ How will they manage reports / investigations?
- ✓ Who will take responsibility for which part of the report processing?
- ✓ What are the procedures for exchange of reports between the hotline and the law enforcement unit, time limitations and details of the exchange.

The nature of the relationship and the details of cooperation will often not be managed in a single meeting but are part of an ongoing process. The positioning of a new hotline will also depend on the existing law enforcement capacity to respond to online CSAM. If there is already a dedicated law enforcement unit with a mandate to investigate online CSEA, the need for a non-law enforcement reporting channel may not seem obvious to them, especially if they have their own reporting mechanism in place. It is essential to build trust between the hotline and the relevant law enforcement unit, as well as inform them about the importance of a hotline. This can take time and should be seen as an iterative process.

Law enforcement should be presented with an overview of the role and value of a non-law enforcement hotline to help:

- ✓ Reduce the workload of law enforcement by filtering out reports of non-illegal content according to the national legislation of the country and referring only relevant reports to law enforcement. Exact figures are difficult to achieve but 60% of the reports hotlines usually receive are not CSAM, so we make sure that law enforcement only gets the 40% that are actually CSAM and need investigating. 60% of the illegal material reported in 2020 to hotlines was previously seen material. This indicates that hotlines save valuable police time, so criminal intelligence officers can spend their time on investigations, identifying perpetrators and safeguarding victims.
- ✓ Engage and educate the public about the importance of reporting online CSAM.
- ✓ Encourage reporting by offering anonymity. A non-law enforcement hotline offering the possibility to make anonymous reports can be a valuable additional source of information regarding online CSAM.
- ✓ Channel URLs hosted in other countries to the relevant country via the INHOPE network for removal at source.
- ✓ Reduce the overall availability of online CSAM material for the public assuring a safer internet.
- ✓ Be a centralised point for online illegal material within the country.

The law enforcement unit may require a copy of all reports sent to the hotline, and they may decide to conduct a quality control on the report assessment by the hotline. However, when designing the workflow of the hotline, a joint report or content assessment training with the relevant law enforcement officers and hotline analysts can help build the confidence necessary. This eventually helps the hotline to act more autonomously and refer reports directly to the international hotline network. An effective hotline ultimately saves times for law enforcement, particularly in countries where there is limited hosting and therefore minimal requirement for local law enforcement to initiate notice and takedown processes.

Most URLs reported to most hotlines will not be subject to investigation in that country. Where the content of a URL reported to a hotline is found to relate to a particular country, the close cooperation between hotlines and law enforcement at national and international level should ensure that the relevant law enforcement unit is notified. Since 2015, INHOPE provides its members with a content hashing and classification tool – ICCAM, that makes confirmed CSAM available to INTERPOL.

#### Personal contact within an institutionalised relationship

To promote successful relationship building and facilitate open lines of communication on an ongoing basis, the hotline could request a part-time dedicated police 'liaison officer' to be the official contact for day-to-day operational issues. For example, an officer could be seconded for half a day each week and this officer could have their own office space at the hotline. It would be extremely valuable to have one committed individual who could be trained up to the right level of expertise and who could manage the working processes between the hotline and the rest of law enforcement. Although this would represent a substantial commitment from law enforcement, it would bring benefits of closer working relationships with industry, as well as education and experience from the international law enforcement community. Despite the importance of specific points of contact and individual relationships, the relationship between the hotline and law enforcement must also be institutionalised so that staff turnover will not affect cooperation between the two.

#### • Law Enforcement Training

If law enforcement officers have access to ICT and are skilled in their use for online child sexual abuse investigations, law enforcement should be invited to take the leading role in training the hotline's content analysts. However, depending on the national context, law enforcement officers in some countries may have little or no experience in ICT and/or investigations of online child sexual abuse images. Police involvement in the hotline will nevertheless be important, so it may be necessary for the relevant police officers to have additional training to be able to support the hotline's activities.

Options for this could include the following:

#### ✓ INTERPOL

National law enforcement should reach out to INTERPOL, which is involved in the delivery of training courses (e.g., skills transference) and other training options for police officers. Relevant police officers would also benefit

from becoming members of the INTERPOL working group so that they can be involved in and learn from related activities, as well as contributing to the International Child Sexual Exploitation Image database (ICSE DB).

#### √ The International Centre for Missing and Exploited Children (ICMEC)

Through its Global Training Academy, ICMEC operates a programme International Law Enforcement Training. Since 2003, ICMEC has been training police officers on the essentials of technology-facilitated crimes against children (for law enforcement and for prosecutors); advanced online exploitation investigations; and advanced technologies. Training is delivered by experienced law enforcement officers from national agencies as well as international organisations such as INTERPOL. These trainings are often sponsored by industry partners and delivered in the relevant country or region. In order to develop the course, ICMEC carries out a pre-assessment of a country or region, to confirm the specific training gaps, and then builds a programme that could cover a range of required areas, such as:

- Online investigations, with case studies: how to deal with digital evidence, how to find the victim behind the image, how to interview the victim.
- o Technology used by offenders types of technology and how are they used.
- o Prosecuting techniques.

#### 5.1.5 Industry, especially hosting providers

Some hotlines may be able to provide access to 'block-lists' of URLs known to contain CSAM or hash-lists (digital fingerprints) corresponding to confirmed child sexual abuse content. This is something which is increasingly in demand from hosting providers to help them keep their platforms free of CSAM. For these reasons, it is vital that the national internet industry understands and shares the objectives of the hotline. Depending on the national context, it might be necessary to invest time and effort in educating key industry players on the nature of the problem, as well as the role that hotlines already play in other countries and how they work with industry. INHOPE can work closely with applying organisations to ensure understanding and to facilitate good relations for future collaboration.

Potential industry partners must understand that the hotline can help them keep their services free of illegal content, as well as protecting their customer care staff from having to look at traumatic content should they receive a report from a user. As a minimum, they must also understand the processes they will need to have in place, in case the hotline alerts them to the presence of illegal content on their services. In some cases, industry will actively contribute to the hotline, whether financially, or with in-kind support such as IT and training.

When trying to gather support from industry, companies should be presented with specific proposals. You should engage with the Internet Service Providers Association if there is one in the country, the national Registry and with the largest national companies. A growing number of multinational companies from the ICT sector have developed global public policy or corporate social responsibility programmes for child online protection. Not only are these an invaluable source

of best practice in industry, but they enable a multiplier effect as these policies and guidelines are introduced nationally and sometimes regionally. Nevertheless, it can be challenging at first to engage industry, especially if this means cooperation with market competitors.

Before engaging with specific companies, seek to understand their general guiding principles. Find an individual within that company who is committed and receptive to ideas and work closely with that one individual. Experience has shown that individual relationships can be crucial to progress.

The hotline needs to build up a proposal for industry players, covering:

#### Any correlation between the hotline work and government mandates

- o Is the government encouraging industry to be active in this space already?
- What does national legislation and regulation say?

#### The hotline's remit and scope

Clearly define the type of content the hotline will be focusing on, and the services it will offer.

#### The benefits it will bring to industry

Corporate responsibility, 'clean' services, staff protection.

#### The kind of support that an industry partner can offer to the hotline, such as:

- o Financial or in-kind support, hardware and software, web hosting, internet connection.
- Technical support to train hotline analysts to understand how they manage content on their platforms.
- Communications support implementing a 'report abuse' button linked to the hotline on their platforms.
- o Promoting the reporting service to their clients through direct messaging.
- Providing free advertising space.
- Sponsoring public awareness events.

Ideally, the hotline will be supported by all players across industry. This should be actively encouraged from the outset through cross-sector representation at the relevant roundtables and working groups. International organisations including GSMA, and UNICEF can provide guidance and support as well as activate their networks to support this process.

However, commitment and leadership by one or two hosting providers is an important starting point. Both they and the hotline organisation (as well as other governmental, civil society and international partners) must encourage cross-industry engagement. Messaging on this issue should be clear: preventing and responding to the online sexual

exploitation and abuse of children is a shared responsibility that should be free of any commercial or brand-related dimension.

The relationship between the organisations running the hotline and industry is a dynamic one. As technology and patterns of connectivity develop, it is essential to maintain good channels of communication and to ensure commitment from both sides to adapt to these changes. It can be helpful to schedule regular meetings as well as an annual event or training.

Working with a hotline organisation to tackle the online sexual exploitation and abuse of children is an opportunity to lead by example for industry companies. The cooperation with a hotline should not be seen as an exercise in branding. Even if there is only one industry partner involved at the time that the hotline service is launched, there should be an agreement in place for additional companies to get involved. A hotline that is 'branded' by one individual company also risks impacting relationships with key stakeholders such as law enforcement, as it may create the perception that the hotline is an initiative of a single commercial business. Where an industry player is the driving force behind the hotline, it should still seek to include other players. Additional brands lend credence to the hotline and may forestall formal legislation. Cobranding may also lead to co-funding.

For both the hotline organisation and industry partners, the following are useful in building and maintaining a strong relationship, and INHOPE can help you with these tasks:

- **Communication**: Have clear and efficient lines of communication the hotline will need to have contact details for the relevant colleague at each national hosting provider.
- Documented procedures: What should industry expect from the hotline, and vice versa? Again, this is to show
  clarity and transparency. Documenting procedures also makes it easier to manage issues relating to staff
  turnover.
- **Regular meetings**: Have physical meetings and briefings invest man-hours in building relationships, showing what the hotline does, sharing its achievements, listening to any concerns that industry has.
- **Problem solving**: Solve problems in closed groups for example, if an industry partner does not actually react to notifications from the hotline as it claims in public, arrange a meeting to discuss the problem and find a solution. 'Going public' with problems should not be used as a means of resolution. This is critical for maintaining trust.
- **Mutual understanding through dialogue**: Consider the industry perspective if industry has a problem with the hotline, see if their views can be accommodated too in the spirit of 'give and take'.
- Commitment to improvement: Always challenge operations to improve them strive to improve the collaboration all the time. The hotline may be fulfilling its remit but consider what else could be done or what could be done better.

# 5.2 Child welfare agencies and civil society organisations as hotlines and as stakeholders

If your country has not yet decided on what kind of organisation will run the hotline, this section is relevant for you. However, if the reader is from the applying organisation, this section can be skipped, and you can go straight to <u>4.3</u>.

It is important to emphasise that there is no single model for a hotline service, as already mentioned. A significant proportion of hotline services currently in operation around the world are operated by non-governmental or civil society organisations with a child welfare or child protection remit. Many have specific expertise in relation to online and offline child protection and may be national franchises of larger global institutions such as Save the Children or ECPAT.

Civil society organisations are often well placed to operate a reporting service for several reasons. These include:

- ✓ Evidence-based and general knowledge of the issues, often based on its own research or research in collaboration with partners.
- Experience dealing with sensitive information and sometimes directly with children and victims of exploitation and abuse.
- ✓ Independent organisation to which the public may feel more secure reporting.
- ✓ Autonomous voice advocating for legal and policy changes.
- ✓ Independent source of accountability for government and the private sector.
- ✓ Pre-existing relationships and experience building relationships with many partners, including across civil society and child welfare institutions.
- Experienced and committed staff with a less frequent, lower turnover than is often seen in governmental and private sector departments.

A lack of sustainable funding is a common concern raised in relation to a civil society organisation operating a hotline service. However, civil society organisations by their very nature are agile and adaptive and often very creative in the way they seek to fund a particular area of their work. In addition, it is important to remember that a civil society organisation operating a hotline service is not and should not be responsible for 100% of the funding needed to provide that service. A hotline service is a collaborative endeavour, and this should extend to the way it is financed. If the hotline service is operated by an organisation from another sector, whether governmental, academic, or private sector, it is important to build strong relationships with civil society organisations for many of the same reasons listed above. Civil Society Organisations can offer a different perspective on the issue, can help provide continuity to the project in the face of staff changes, and can sometimes reach populations that are harder to reach for governments and law enforcement.

If the hotline is an initiative of industry (for example, a hotline operated by an internet service providers' association), a Civil Society Organisation can offer subject-matter expertise that may not be present at the start of the hotline's life. It

can also influence efforts to change legislation and they can be a crucial partner in promoting the reporting service to the general public.

Civil Society Organisations are well placed to judge the degree and nature of awareness-raising activities that will be required for the hotline to succeed, and to run awareness-raising campaigns in a similar or related area.

### 5.3 Funding and sustainability

Ensuring adequate and sustainable funding sources is critical. Hotlines are unlikely to fail due to lack of relevance, public interest, and support, but occasionally they have failed due to lack of sustainable funding or to unforeseen economic downturns.

Consideration should be given to diversity of funding sources from the start. A hotline service funded by multiple sectors and/or organisations will be more resilient. This also means that the cost of supporting a hotline service is shared among stakeholders, which re-enforces the collaborative nature of the undertaking. In many cases, however, funding and relevance are co-dependent. The relevance of the hotline service is both the origin and an outcome of its creation. Building the business case for a national hotline will be important for its longer-term survival.

#### What is the cost of setting up and running a hotline?

This is a common question from all sides in the early stages of a hotline development project. In reality, the actual set-up and running costs of a hotline will depend on several variables.

#### These include:

- ✓ Local costs in the country of operation.
- Existing infrastructure within the organisation that will operate the hotline service.
- ✓ Size and scale of the planned operation.
- ✓ Standing and new commitments of financial or in-kind support (e.g., office space, connectivity) from local industry partners or international partners.

However, a business model will probably need to account for most of the following items:

- Personnel: recruitment, training, salaries, counselling, insurance (e.g., to cover personal injury claims from staff).
- ICT: website development and maintenance costs, phones and phone lines, internet connectivity, computers/printers/photocopiers/fax, local Report Management System (unless you use Report Box which is free to organisations looking to become members of INHOPE), security software etc.

- Office: premises, utilities, security, insurance; the hotline desks and computers must be placed in a secure room, accessible and visible only to trained and authorised staff.
- Additional: Promotion/PR/advertising collateral, legal counsel, accountancy/financial planning support.

In many cases, the hotline service will be run by an existing organisation with a broader remit and activities. These costs will often not fall solely upon the hotline service but will be part of the overall costs of the organisation. Nevertheless, there are cost implications to adding any new service or activity to the work of an organisation, and these must be given careful consideration in the planning phase. Organisations can consider seeking in-kind donations for items such as hardware and software.

#### 5.3.1 Applying for government funding

Governments can be a useful source of funding. Governmental funding visibly demonstrates government support for the hotline, thereby enhancing credibility.

Things to consider if applying for government funding include the following:

- International dimension: It might be advisable to give evidence of becoming an INHOPE member in order to give the international context of the hotline.
- Cross-sector partnerships: If applying as a corporate entity, you need to show that your organisation will offer seed funding and that you have other partners involved. It is unlikely that a lone industry player will succeed in gaining government funds. Assuming an NGO is also involved, it is preferable that the industry player is not the lead applicant. Let the NGO be the applicant and request funding on the basis that Company X has promised e.g., 50 per cent and government support is sought for the remainder.
- Consortium structure: In some countries, it may be easier to apply for money or funds as a consortium with other organisations which are running related 'Internet Safety' initiatives. For example, applying for a complete child online safety/protection/education package not just a hotline can be a more powerful approach in certain circumstances, provided that each of the parties within the consortium has credibility.

#### 5.3.2 Internet industry funding

The industry benefits directly from the hotline's ability to help internet service providers keep their services free from illegal content and to protect their staff from having to deal with issues relating to illegal content themselves. Therefore, it is logical for an industry company to fund the national hotline. There are also additional benefits such as positioning and corporate responsibility. Industry is instrumental in providing funding in a few markets.

#### Funding from unrelated industries and/or private donors

It may be possible to secure funding from organisations that do not have a direct role or direct benefit from the hotline service. These could include:

- Non-internet industry' private sector sources: These would not expect to use the hotline 'services' but may nevertheless be willing to contribute funding to a hotline as part of their corporate responsibility programme. Before accepting the donation, it is important to understand the motivation and any expectations the company may have in terms of publicity or branding. This will help avoid misunderstandings and protect the mission and reputation of the hotline.
- Charitable foundations and other grant giving organisations: These may have funding for projects that address the sexual exploitation and abuse of children or even specifically online sexual exploitation and abuse of children. Indeed, there is increasing understanding of and concern about the linkages or blurred lines between 'online' and 'offline' CSAM.
- Private benefactors: These can also be a source of funding. However, try to avoid over-reliance on this type of
  funding. Whilst the internet industry has a vested interest in the continued success of the hotline, non-related
  industries and private individuals might not have the same long-term commitment.

Before seeking or accepting private funds, the origin of funds should be established, and any potential reputational risks identified. For example, consider:

- ✓ What kind of company or individual is offering funds?
- √ What, if any, are the 'public relations' or other motivations for offering funding to a hotline
- ✓ How might this impact the hotline?