Mobile Alliance Against
Child Sexual Abuse Content

INTERNATIONAL ASSOCIATION OF INTERNET HOTLINES
INHOPE

GSMA in association with INHOPE

Hotlines:
Responding to reports of illegal online content

A guide to establishing and managing a hotline organisation

October 2013

Contents

Founding and developing a hotline organisation for the reporting of illegal online content

In recent years, internet usage and connectivity have grown rapidly. The internet has changed the way we communicate, the way we do business and ultimately the way we live. Although society benefits greatly from the opportunities afforded by the internet, sadly there are also those who use this technology for illegal activities, in particular spreading Child Sexual Abuse Material (CSAM).

The International Association of Internet Hotlines (INHOPE) coordinates a network of internet hotlines all over the world, supporting them in responding to reports of illegal content to make the internet a safer environment. INHOPE members operate a public hotline to receive complaints about apparent illegal content from the public. Teams of analysts then assess the content in accordance with their national laws and if they consider the content to be illegal they trace the material to a hosting country. If the content is illegal in the hosting country then the national hotline takes steps to have the material 'taken down' in consultation with their law enforcement partners and in partnership with mobile network operators and internet service providers.

This is a global problem, requiring a unified global response. As our network of hotlines continues to expand internationally, we are increasingly able to field such a response.

We welcome this Guide from the GSMA and value the role it will play in growing our network by supporting the creation of new hotlines in countries that do not yet have such a facility available.

Russell Chadwick
Executive Director
INHOPE Association

Chapter 1
Purpose and structure of this document

As part of its ongoing commitment to fighting online child sexual abuse content and, in particular, to helping its members realise the objectives of the Mobile Alliance Against Child Sexual Abuse Content, the GSMA has worked with INHOPE, Save the Children, ECPAT, IWF, Net Safe Latvia, Meldpunt, ICMEC and Interpol to collate information which will help organisations build fully-functioning hotlines in countries where no such facility is currently in place.

This information is presented in the document below, and is structured as follows:

The role of 'hotlines'	This section provides a brief summary of the key role played by hotlines in combating the presence of illegal online content, such as child sexual abuse content.
Creating a hotline organisation	This section considers the key elements for getting a hotline facility "up and running", such as: core partners (e.g. government, law enforcement), sources of funding and sustainability, and defining the role and remit of the hotline organisation.
Logistics	This section details practical information designed to help inform the planning process – it covers infrastructure requirements and staffing considerations.
Operations	This section provides good practice learnings and working examples of hotline processes for operational issues, such as: managing reports coming from internet users, managing reports coming from industry, analysing findings and trends, collaborating with national / international law enforcement agencies, and so on.
Communication	This section offers examples of successful approaches to communication and messaging to stakeholders, including raising awareness of the hotline and its remit to the general public.

The documentation is not intended to offer any judgement of which approaches are "best" – rather it is designed to support organisations which are looking to introduce similar initiatives and processes by providing a range of points of view and approaches, some of which may be also appropriate for use by other organisations.

Chapter 2
The role of 'hotlines'

2.1 Background

The first hotline for reporting child sexual abuse content was set up in the Netherlands in June 1996 as a joint initiative between industry, government and law enforcement. This was followed by similar initiatives for reporting illegal content in Norway, Belgium and the UK before the end of the year. Since then, many EU countries have created hotlines supported in part by EU funding and INHOPE (the International Association of Internet Hotlines – see below), the rapidly expanding umbrella organisation for hotlines, now has 44 hotlines in 38 countries across the globe.

The role played by national hotlines in terms of taking reports of illegal content – in particular, child sexual abuse content – and helping to develop and support national protocols for Notice and Take Down (NTD) processes by identifying or confirming the presence of such content, is a key first line of attack in combating illegal content online.

2.2 INHOPE

INHOPE[1] is the global association of national hotlines for the reporting of illegal online content. By sharing knowledge, information and best practice, INHOPE and its members are working to tackle the global problem of illegal content online.

The mission of INHOPE is to support and enhance the performance of internet hotlines around the world; ensuring swift action is taken in responding to reports of illegal content in order to make the internet a safer place.

To achieve this mission, INHOPE has five specific objectives:

1 To establish policies and best practice standards for hotlines and encourage exchange of expertise among members through fostering good working relationships and trust.

2 To ensure rapid and effective response to illegal content reports around the world by developing consistent, effective and secure mechanisms for exchanging reports between hotlines internationally and ensuring a coordinated approach is taken.

3 To expand the network of INHOPE members around the world by identifying and supporting new hotlines to become members by providing consultation and training to meet best practice standards.

4 To promote a better understanding of the work of hotlines to policymakers at an international level, including government, law enforcement and other related bodies, with the aim of achieving better co-operation internationally.

5 To raise awareness of INHOPE and member hotlines with key stakeholders as well as the general public as a "one stop shop" for global reports of illegal content from around the world.

1 https://www.inhope.org/

Chapter 3
Creating a hotline organisation

3.1 Getting started

This document provides information which will, in general terms, apply to hotlines across the world.

The key starting point, however, for any initiative seeking to found a hotline will be to get to grips with the particulars of their national context – developing a thorough understanding of the local legislation, the cultural expectations, the likely scale of the problem, and so on. The Family Online Safety Institute's (FOSI) Global Resource and Information Directory (GRID), or FOSI GRID[2], provides up to date information on internet safety by country and region. See also ECPAT's Global Monitoring Report on the Status of Action against the Commercial Sexual Exploitation of Children for a country by country overview of activities[3], and ICMEC's Model Legislation and Global Review for a high level comparison of legislation[4].

Working with one or more established national NGOs dealing with issues of child welfare – potentially but not necessarily including online safety – could be a good place to start. A local NGO with experience in child sexual abuse issues will not only have a good understanding of the scale of the problem in the particular country and related national legislation, but they may be able to help the developing hotline organisation to navigate law enforcement procedures, find the right contacts within government and industry, and so on.

Specific professional advice should be sought with regard to legislation which bears directly on hotline activities – 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 job?
- Are there issues around data storage (e.g. relating to the URLs, files, reporters ID / IP address)?
- Are there issues around maintaining reporter 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? – Is there a requirement for a hotline to be managed under the auspices of a national authority (e.g. film classification board, a media and communications authority etc)?

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.

2 http://www.fosigrid.org/
3 http://www.ecpat.net/A4A_2005/index.html
4 http://www.icmec.org/missingkids/servlet/PageServlet?LanguageCountry=en_X1&PageId=4346

Having established the national context, the hotline should seek to visit an existing hotline with a similar cultural context – ideally key staff should be given the opportunity to spend time 'shadowing' the working day in an existing hotline with 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 – something that is unlikely to be the case at well-established hotlines such as the CyberTipline[5] or the Internet Watch Foundation[6]. Whilst it may be of interest to visit such hotlines to learn about the operational aspects of running a hotline, be aware that as these hotlines are well-established, levels of investment, staffing and so on, are on an entirely different scale to those which will be necessary for a new hotline (see Section 4: Logistics for more detail on this subject).

For example, when Save the Children was looking to set up a hotline in Italy, in 2002, the team responsible for setting up the hotline was effectively starting from scratch. They had no technical background, they had never seen an illegal child sexual abuse image. However, as they were working within the European context they had access to EU funding and the opportunity to learn from and build upon activities in other countries. At the beginning of the process, they spent 2 – 3 days visiting the Danish hotline to see how it worked: this afforded the opportunity to discuss the hotline structure and operational procedures with their Danish colleagues, and they were also able to shadow the hotline analysts as they worked – so they were properly briefed and mentally prepared before being exposed to images, and so that they could learn how to manage reports, investigate images, take appropriate action, and so on.

Contact INHOPE who will be able to help members (and hotlines in the process of gaining membership) to find a suitable match.

3.1.1 Additional options for smaller or emerging markets

Organisations from smaller countries or emerging markets with lower levels of internet take up may wish to consider two additional options:

- INHOPE Foundation – the INHOPE Foundation is the charitable arm of the INHOPE Association of Hotlines. It has a remit to help support aspiring new hotlines where there is greatest need.

- IWF International – IWF analysts process reports of child sexual abuse content made through locally-branded webpages, on a cost-per-report basis.

Further details on these two options can be found in Section 7: Additional options for emerging markets.

5 www.cybertipline.com, USA
6 http://www.iwf.org.uk/, UK

3.2 Working with external stakeholders

It is not possible for hotlines to operate successfully in isolation – indeed, the INHOPE statutes require that a hotline seeking INHOPE membership must establish sound working relationships with law enforcement, the internet industry, government and child welfare agencies.

The support and engagement of the following external stakeholders, dealt with in turn below, is of great importance to the successful development of a new hotline:

- Government
- Law enforcement
- Internet industry
- Child welfare agencies
- Other hotlines / INHOPE

Consider holding a conference, early on in the start-up process, inviting all the relevant stakeholders, to discuss the nature of the problem and proposals to tackle it through the national hotline and, ideally, include speakers from INHOPE or an existing hotline. This is a useful way of educating all parties, ensuring and demonstrating support from government and law enforcement, and getting industry players who have not previously had much exposure to – or experience of – online child sexual abuse content involved too.

3.2.1 Government

Government support for the hotline initiative will be critical to its success in a number of ways: it will be vital in terms of managing any potential issues related to navigating or re-defining legislation, it will provide credibility in the eyes of other key stakeholders and the general public, it may lead to government funding contributions and it will 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 communications / technology (e.g. Ministry of Communications) – particularly if there is an active online safety programme, or equivalent, which is headed up by this area. This department may play a particularly valuable role in promoting the hotline to the public as part of its wider safer internet activities; it will probably also be the department that will be in a position to decide whether a self-regulatory (as opposed to a formally regulated / legislated) hotline initiative is deemed adequate within the national context.

- The department with a remit for law enforcement (e.g. Ministry of Justice) – this department will be able to assist with legislative issues (assessment of what is illegal, etc) and so on, as well as endorsing involvement and resource from law enforcement. The hotline will also need a written agreement with this department (unless the agreement can be made directly with law enforcement) that the hotline employees have the right to receive reports and look at the content, etc – potentially by having the hotline's operational procedures formally approved by them.

Engage with both departments as soon as the full initial hotline proposal has been developed – however, if at all possible, ensure that the relevant law enforcement unit is contacted in parallel with (not subsequent to) your engagement with the governmental justice department (see 3.2.2 *Law Enforcement*, below).

In addition, the Law Enforcement Agency (LEA) / hotline will need to collaborate with the national data protection agency to understand any implications for the hotline and its proposed activities and processes.

For further discussion on applying for government funding, please see 3.3 *Funding and Sustainability*, below.

3.2.2 Law enforcement

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

- Aim to get law enforcement involved early on – depending on the market context, the issue of online child sexual abuse content may by higher or lower on the list of the national LEA's priorities. If child sexual abuse content is not a priority area at present, be prepared to sensitise law enforcement colleagues to the scale of the problem, the wider international backdrop, and the ambitions of the national hotline within this context. INHOPE will be able to provide up-to-date statistics (e.g. ages of children, breakdown of commercial versus non-commercial content, and so on) to support the presentation – you may also want to invite an INHOPE representative to share their insights at an initial meeting with LEA.

- Try to find the appropriate unit – there is a unit for child crime in most countries (which might also cover issues relating to domestic violence, sexual assault, family, and so on), and there may be also be a cybercrime unit that would be expected to lead on this. It may be difficult to find an obvious entry point as child exploitation online does not yet have a typical organisational home – is it a 'cybercrime' which should be handled by the cybercrime unit or a real crime with 'cyber evidence' that should be handled by the child unit? If it is unclear from an external perspective, the relevant government department should be able to direct you. However, be prepared for the eventuality that it is not clearly defined and that cases are shared somewhat haphazardly across departments.

- Aim to engage at the most senior level possible to gain support and traction for the hotline 'from the top down' – if attempts to reach a senior figure in the units outlined above are unsuccessful, consider reaching out to Interpol, which covers Child Sexual Exploitation on the internet through its THB (Trafficking in Human Beings)[7] function. Interpol may be able to assist by brokering 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 "block list" of known illegal child sexual abuse image URLs, which will be of relevance to industry partners seeking to introduce this type of blocking.

- Avoid a situation where government has become engaged and active in the process before law enforcement has been contacted, to prevent a set of circumstances whereby 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.

- Be prepared, in less developed countries, for LEAs which are understaffed and lack ready access to a range of equipment, including phone lines and so on – if this is the case, manage your approach and expectations accordingly.

Having made initial contact, set up a meeting to explain the plans for the hotline and a proposed approach for working with law enforcement. It is paramount to take a credible and reasonably developed hotline proposal to the LEA, even at the initial meeting. If possible, aim to have the following documented or in place when you make initial contact (even if it is expected that they will be further developed in collaboration with the LEA once it is involved):

- Information on context, scope and ambitions for the hotline – effectively the 'business plan'.

- Draft proposals for working together and an invitation to become involved in the development process – in terms of the ongoing relationship with law enforcement, the parameters will need to be established by negotiation: what are the priorities? How much support are they able to provide? How will they manage reports / investigations? Who will take responsibility for what? Etc. This is an opportunity to present a 'straw man' for discussion.

- Documented and transparent procedures that the LEA can accept, even if they may want to help build on them further once there are more involved in the process – these would include approaches to security, staff welfare, processing reports, and so on (see sections 4 and 5 for further information on these).

- Secure offices, with no access for anyone not involved in the hotline – although you may wish to hold the initial meeting at the LEA's offices, invite them to visit the hotline premises at a subsequent meeting so that they can see your operations for themselves.

7 http://www.interpol.int/Public/THB/default.asp

If law enforcement officers have ready access to ICTs – and are skilled in their usage – as well as experience in online child sexual abuse investigations, law enforcement should be invited to take the leading role in training the hotline's content analysts (see Section 4.2 *Staffing* for further information on this).

However, depending on the market context, law enforcement officers in some countries may have little or no experience in the area of 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 in order for them to be able support the hotline's activities. Options for this could include the following:

- National industry partners and industry associations could provide training in ICTs as part of their contribution to the hotline.

- ICMEC – the International Centre for Missing and Exploited Children[8] – runs courses for law enforcement officers which are tailored to the needs of specific country or region. These need to be sponsored – usually by industry partners – and are supported by organisations such as Interpol, and delivered in that 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:
  - Technology used by offenders – which technologies, how are they used
  - Online investigations, with case studies: how to deal with digital evidence, how to find the victim behind the image, how to interview the victim, etc
  - Prosecuting techniques
  - International collaboration

To discuss options for developing a bespoke training course of this kind, ICMEC can be contacted through: Guillermo Galarza, Program Director, Training Programs and Outreach, ggalarza@icmec.org.

- **Interpol** – national law enforcement should reach out to Interpol which offers courses (e.g. skills transference) and training options for police officers; the 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)[9].

- **INHOPE and hotlines** – new hotlines who are applying to become members of INHOPE can reach out to INHOPE with requests to visit hotlines in comparable markets, shadow analysts whilst they carry out image assessment, and see how hotlines work with law enforcement in comparable markets. INHOPE also offers workshops to applicant members (see 3.2.4) which could be attended by the hotline's law enforcement contact(s).

INHOPE operates the Vanguard programme – which enables new or emerging hotlines to attend INHOPE member meetings to mix with and learn from established hotlines.

INHOPE also administers the Mentor programme to help new hotline initiatives get a good start by pairing them with an experienced 'mentor' hotline.

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 his or her 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 (particularly in countries with resource issues or where child sexual abuse content is not considered to be a priority), it would bring benefits of closer working relationships with industry, as well as education and experience from the international law enforcement community.

8 www.icmec.org
9 http://www.interpol.int/Public/Children/Default.asp

Further reading

The Council of Europe has produced a set of guidelines which were designed to be used "to help law enforcement and service providers in any country around the world to organise their cooperation against cybercrime while respecting each others' roles and responsibilities as well as the rights of internet users." The guidelines[10] could help inform proposals for working relations between hotline / law enforcement and industry.

The same guidelines are available in French, Arabic, Georgian, Portuguese, Romanian, Russian, Spanish or Ukrainian[11].

3.2.3 Internet industry

One of the major benefits of having national hotlines in place is that they facilitate the removal of illegal content that is being unwittingly hosted by service providers in that country. Similarly, hotlines may be able to provide access to "block-lists" of URLs known to contain child sexual abuse content – something which is increasingly in demand from ISPs. Clearly, therefore, it will be vital that the national internet industry players understand and share the hotline's objectives.

Depending on the market context, it might be necessary to invest time and effort in educating key industry players on the nature of the problem, the role that hotlines already play in other countries and how they work with industry. 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 customer. 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.

Ideally, industry will actively contribute to the hotline – whether financially, in terms of expertise, or in other ways. When trying to gather support, take specific proposals out to the industry. Engage both with the industry association if there is one (this will help to build credibility as well as show transparency) and with the major individual companies in the market. The nature of the market in question will make it clear who should be targeted – for example, in the Philippines, the ECPAT hotline made a point of reaching out to internet cafes too.

Before engaging with specific companies, seek to understand their general guiding principles and 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 matter.

Build up a proposal that you can take to industry players, covering:

- Any correlation between hotline proposals and government mandates – 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, and so on.
- What kind of support that particular player can offer to the hotline – everyone has a role to play and some expertise that can be valuable. Be clear with industry players about what their role could be – is it funding? Resources? ICT Training? Infrastructure (e.g. SMS promotion)?

In reality, it is unlikely that all of the target internet service providers will engage at the same time – you will need a leader, but it is enough to have one or two key players actively involved at the start. Once the hotline is up and running, it can be easier for other players to follow once they can see what is involved. However, you need to be able to show that you have tried to get other industry players involved – even if they are not keen to join at the start – and keep the door open for them to join when they are ready.

With regard to branding, beware of launching a hotline which is 'branded' by one individual company – even if that company is the only one engaged at the time of launch. Such an approach 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. It would also run counter to the long term best interests of a hotline: the goal must be to build one national civilian hotline, which aims to get other stakeholders involved over time, and to avoid several

10 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf
11 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp

hotlines all being set up by different players. If an industry player is the driving force behind the hotline, they should still seek to include other players – additional brands lend credence to the hotline and may forestall formal legislation, and co-branding may lead to co-funding.

In terms of working successfully with industry on an ongoing basis, and working with industry to make the hotline the best it can be, the following are key considerations:

- Have clear and efficient lines of communication – the hotline will need to have contact details for the relevant colleague at each ISP.
- Document procedures – what should industry expect from the hotline, and vice versa? Again, this is show clarity and transparency. Documenting procedures also makes it easier to manage issues relating to staff turnover.
- Have physical meetings and briefings – invest man hours in building relationships, showing what the hotline is doing, sharing its achievements, listening to any concerns that industry has, etc.
- Solve problems in closed groups – for example, if an industry partner does not actually do what it claims it does in public in terms of reacting to notifications from the hotline, meet 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.
- 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'.
- Always challenge operations to improve them – strive to improve the collaboration all the time. The hotline may be fulfilling its remit, but what else could be done (e.g. URL blocking?) or what could be done better (e.g. promotion)?

3.2.4 Child welfare agencies/NGOs

Child welfare agencies and non-governmental organisations will be able help the hotline gain traction with key stakeholders, from government to the general public, as well as give valuable insights into the status of child sexual abuse content initiatives during the hotline development process.

It may be preferable to connect with more than one national NGO partner. Seek to find organisations which:

- Have experience in child sexual abuse issues and will be able to give insight into the kind of demand that may come up and the level of the problem in the country.
- Can judge the degree and nature of awareness-raising activities that will be required for the hotline to succeed, and, ideally, already run awareness-raising campaigns in a similar or related area.
- Work to influence legislation in this area.

3.2.5 Other hotlines/INHOPE

For security reasons, INHOPE and its members can only work closely and collaborate fully with other members. However, it is assumed that any organisation building a hotline from scratch will do so with the aim of becoming an INHOPE member and there are a number of benefits to belonging to the INHOPE family of hotlines, including:

- Access to INHOPE training courses, e.g. specific courses for new hotlines (including how to use the INHOPE report management system), advanced tracing techniques, media training, staff welfare, and so on.
- One continuous INHOPE contact to provide support and advice, as well as access to the INHOPE hotline 'mentoring' programmes for new hotlines. The Mentor programme is where an experienced INHOPE member hotline acts as mentor to a new hotline initiative. This programme has been in operation for many years and is extremely beneficial the recipients and rewarding for the Mentor. Most INHOPE current members benefitted from this system, as they were starting the INHOPE membership path.
- Free use of the INHOPE bespoke report management system which enables hotlines to record and access their own data: INHOPE has developed a URL database which

reduces the duplication of reports across the network and reports passed to law enforcement. Furthermore it enables INHOPE to compile unique statistics on the proliferation of images of child sexual abuse on the internet.

- The option to request international data and statistics for comparative analysis.

- Ongoing inter-hotline operational collaboration through a central INHOPE reporting system.

Hotlines who are not members of INHOPE can contribute reports of illegal content to an INHOPE member hotline, however, they will not receive information in exchange – again, this is purely for security reasons.

INHOPE expects its members to abide by INHOPE best practices and maintain the INHOPE standard, to accept other people's cultural differences, and, of course, to treat information as confidential.

3.3 Funding and sustainability

Ensuring adequate and sustainable funding sources is critical – experience to date has shown that hotlines have never failed due to lack of public interest and support, but occasionally they have failed due to lack of sustainable funding.

3.3.1 Hotline costs

Actual running costs of a hotline will depend on a number of variables, such as local market costs, whether some infrastructure costs (e.g. office space, connectivity, etc) can be supported by local industry partners, size and scale of the planned operation, and so on, but a business model will probably need to account for most of the following cost 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, Report Management System (although the INHOPE RMS is available free to hotlines applying for INHOPE membership), security.

- **Office:** premises, heating / electricity / etc, security, insurance.

- **Additional:** Promotion / PR / advertising collateral, legal counsel, accountancy / financial planning support.

3.3.2 Applying for government funding

Governments can be a useful source of funding, and getting funding commitment from the government affords secondary benefits in terms of visibly demonstrating government support for the hotline, thereby enhancing credibility.

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

- It might be advisable to give evidence of becoming an INHOPE member in order to give the initiative international context and credibility. Similarly, do not assume that the international context is understood – provide "evidence" (e.g. findings from the ECPAT world conference)[12].

- 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 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.

- In some markets, 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. (See case study below, which combines work on education / moderation standards with hotline proposals).

Case study: Excerpts from Save the Children Denmark's (SCDK) application for EU funding, showing proposed role, remit and scope

The SCDK internet hotline will continue its long established operational work, acting as a civilian referral hub for alleged child sexual abuse material online. It will accept information on child abuse material from the Danish public as well as international contacts that wish to either submit generic referrals or those specific to material apparently hosted on Danish servers.

The hotline covers the following online services: WWW, Peer-2-Peer, chat, newsgroups, instant messaging, bulletin boards and social networking sites and e-mail. It will ensure that technical measures will be developed so as to allow for mobile internet clients to be able to report to the hotline.

The hotline verifies and assesses the content of all received referrals prior to further processing them. In case of suspected child sexual abuse material is found, the apparent origin will be traced and information will be forwarded to the relevant collaborators according to Best Practice stipulated by INHOPE and implemented by the hotline.

- **Work package title:** Hotline operational work
- **Objectives:** Operate a hotline for Denmark to receive information from the public relating to illegal content on the internet
- **Tasks:**

1 Set up and maintain a facility for online reporting of illegal content and/or activity on the internet and new online technologies.

2 Draw up a manual of procedures in cooperation with law enforcement authorities and in accordance with best practice guidelines drawn up by the network.

3 Deal rapidly with complaints received.

4 Exchange specific information on identified illegal content with other members in the network.

5 Actively inform users of the hotline's scope of activity and how to contact it.

6 Recruit, train and supervise staff. Open a dialogue on staff welfare and find ways to achieve this.

7 Gather and analyse statistics based on the network template to track performance and establish trends.

3.3.3 Internet industry funding:

There is logic to industry helping to fund hotline activities, as the industry benefits directly from the hotline's ability to help ISPs keep their services free from illegal content and to protect their staff from having to deal with issues relating to illegal content themselves. There are also additional benefits to be gained from supporting a hotline which relate to positioning and corporate responsibility. Industry is instrumental in providing funding in a number of markets.

Case study: IWF, UK – Industry funded

The Internet Watch Foundation (IWF) is the UK's hotline for reporting illegal online content. It is a self-regulatory, independent industry-funded body, supported by the UK Government and national law enforcement agencies. Its member companies are highly respected enterprises and include ISPs, mobile operators, filtering companies and content service providers. Many of these companies are international and based outside of the United Kingdom.

There are two categories of IWF membership: Full and Associate. Full members are defined as those able to take down online content (e.g. ISPs, content providers, MNOs) and Associate members are companies that support the objectives of the IWF but do not host online content (e.g. industry bodies such as the GSMA). All membership applications must be approved by IWF Board.

The IWF offers a number of services to its industry members, including NTD support, provision of list of 'keywords' often used by individuals seeking child sexual abuse content, and a dynamic list of URLs which contain child sexual abuse content so access to these URLs can be blocked. Membership starts at £5,000 per annum for organisations who wish to gain access to the full range of services and benefits available from the IWF, and many large international companies pay annual subscriptions in excess of £20,000.

The IWF also received funding from the European Union through the Safer Internet Programme.

3.3.4 Funding from unrelated industries and/or private donors:

It may be possible to secure funding from 'non-internet industry' private sector sources, who would not expect to use the hotline 'services' but who are nevertheless willing to contribute funding to a hotline as part of their corporate responsibility programme. Similarly, private benefactors may wish to contribute funding.

Before seeking or accepting this type of funding, it is worth considering whether there are any risks of credibility issues in this instance (What kind of company / individual is it? What, if any, are their 'PR' motivations for offering funding to a hotline, and how might this impact on the hotline?). Also, safeguard against over-reliance on this type of funding – whilst the internet industry have a vested interest in the continued success of the hotline, non-related industries and private individuals might not have the same long term commitment.

3.4 Defining the hotline's role and remit

It is advisable to keep the hotline's focus as narrow and specific as possible – ideally focusing it purely on *illegal child sexual abuse* content.

This is partly to ensure clarity of messaging and thus to prevent the hotline becoming a 'catch all' for reports of any content that users may deem to be unsuitable (as opposed to *illegal*), and partly to instil confidence in the hotline because it can be precise about the definition of illegal content. The hotline should already have outlined its planned remit and scope in any proposals that are taken to government and law enforcement, so that the nature of support being requested is clear and contained.

In terms of governance, the hotline must be seen to be independent (e.g. no political bias) but with clear reporting lines – for example, into the Ministry of Justice, or a working group comprising the Ministry of Justice, teachers groups, NGOs, etc.

Chapter 4
Logistics

4.1 Infrastructure

4.1.1 Hardware

Start-up hardware requirements are essentially to have a computer with internet access, a server for the website and a separate server or computer for the Report Management System (RMS), which, ideally, will be standalone so that reports can come into it, but nothing can be sent out. The RMS must not be stored 'in the cloud'.

4.1.2 Software

Hotlines will need to use a database or Report Management System (RMS) for tracking reports and their handling. It is possible to create one using standard software (e.g. working MS Access sample systems) or to work with bespoke software (see case study below), however INHOPE now provides its members with a free RMS which is effectively a smaller version of the database INHOPE uses to reduce the duplication of reports across the INHOPE network and to law enforcement, and to compile unique statistics on the proliferation of images of child sexual abuse on the internet.

Case study: Sweden

The ECPAT Sweden office uses specifically developed software, NetClean Analyze, for the analysis of the reports. The custom-made software (which can be provided to other hotlines through ECPAT Coordination) enables the analyst to process a large number of reports and also avoids duplication by ignoring similar reports. The software also connects with common databases linked to hotlines operating similar software, and can thereby flag sites that have already been reported to other hotlines. Further information on the NetClean Analyze Suite can be found here: http://www.netclean.com/en/analyze/for-law-enforcement/read-more/.

It is important to have firewalls and a very good anti-virus system in place, which should be working at all times. Computers which are used for viewing illegal images should be checked / scanned regularly (at least once a month). A good example of an open source tool for "cleaning" the computer is CCleaner[13]. Some hotlines also use a software virtual computer to protect their own computers from being infected by malware when viewing suspect sites.

Additionally, hotlines could consider setting up a "Tor" network[14] or equivalent, for when they are accessing sites containing illegal content. This will prevent sites visited from watching the hotline's internet connection and learning its physical location.

Thought should be given to how confidential information is shared with law enforcement – one option is to send encrypted information via email.

4.1.3 Investigation tools

INHOPE offers its members courses on tracing IP addresses and websites using a variety of open source tools.

The following are examples of the types of tools used by hotlines:

- Who is – to look up domain names
- Visual route – to look up IP address routing
- Robtex – provides AS number and ISP
- Ip2location.com – provides a map of the IP address in use
- http://centralops.net/co/
- http://www.domaintools.com/

As a matter of best practice, when determining domains, at least two different tools should be used – and if they return different information, then additional tools should also be used.

13 http://www.piriform.com/ccleaner
14 http://www.torproject.org/

4.1.4 Office set-up and controlled access

The work station of a hotline analyst should be positioned so that no one can see his / her computer screen / monitor by accident, while passing by. Ideally, the work should take place in a room that has a door which can be locked, and a warning sign (e.g. "knock before entering") should be placed on the outside, to prevent inadvertent exposure to illegal content. Further information on working environment can be found in 4.2.3, below.

4.2 Staffing

4.2.1 Team: structure, recruiting and training

Team size and structure will depend somewhat on the volume of reports coming in, but the initial team should consist of one content analyst and one communications manager (i.e. individual responsible for managing policy / politics / communications and so on):

Content analyst(s):

In the region of 1000[15] reports in the first year of operation would be considered a promising start. As a typical content analyst will be able to deal comfortably with 100 reports a week (20 reports per day is 'very manageable'), only one content analyst will be required to get the hotline facility up and running. The 'tipping point' at which another analyst should be hired is when enough reports are coming in that they cannot be dealt with within 24 – 48 hours of receipt.

When hiring the first analyst, it is worth looking for an individual who has the potential to become the lead analyst / hotline manager as the organisation grows.

The IWF job description below is a good starting point – however, bear in mind that the description is for a 'pure' content analyst who will be working in a busy hotline organisation that has been running for years. When starting off, it is likely that the first content analyst will have excess capacity and will therefore also be able to manage additional tasks – so the job description should take account of this. For example, in one country with a small but established hotline, receiving only around 15 – 20 reports per month, the two hotline employees also run an 'awareness node' and through this they also go into schools to teach children about safe internet usage.

In general, a content analyst should:

- have a basic interest in and understanding of how websites work – for example they may have built their own website or attended evening classes on web design – and the fundamentals of online security / personal security on the web. However, they do not need to be a technical 'expert'.
- have an interest in and an ability to grasp the legal issues involved with classifying content and managing reports be comfortable presenting to stakeholders (e.g. law enforcement colleagues) – this will include the ability to describe and discuss graphic content in a factual and pragmatic tone.
- have 'life experience' and maturity – new graduate recruits have been shown to have higher turnover than more mature recruits. Note: other than 'life experience' being valuable, make no other assumptions about potential recruits. For example, experience from a number of hotlines has shown that young mothers returning to work can be very successful content analysts – even though it may be tempting to assume that such a role might be too 'traumatic' for them, this is not necessarily the case.

In terms of assessing the candidate's temperament for the job, the interviewer's personal instinct plays a valuable part. Ask questions like "why do you want to work in this field?"; "how do you think you will cope with the reality of looking at images of children being sexually abused?" and look for measured and realistic responses. Be wary of 'extreme' answers such as "I think that paedophiles should all be hunted down and shot".

The final stage of recruitment should also be used to give the candidate the opportunity to test for themselves whether they are temperamentally suited to the role. Once the preferred candidate for the role has been selected, all available police checks should be carried out, and (if appropriate – seek local legal advice) the candidate should be asked to sign a 'temporary' contract acknowledging that they understand the nature of the content they will be viewing and assessing.

The candidate should then be invited in to spend an hour in a room with an experienced analyst or law enforcement officer, looking at the type of content and images that they would be examining in their day to day role as a hotline

15 Note: typically around one in four reported URLs are actually found to contain illegal content upon investigation.

content analyst (including extreme adult material and content involving children of different ages). It is not necessary to ask the candidate to describe the acts / activities depicted at this stage, but it is important that they are exposed to real content and encouraged to describe other relevant information that would be noted during a standard investigation of a report, e.g.: "What can you see on the shelf behind the child?"; "What type of plug socket is that?" etc.

It should be made clear to the candidate that they are being offered the job, but that this session is their opportunity to be sure that they definitely want to accept it. Carry out this final 'working session' at the end of the working week, and give the candidate the weekend to think it over – ask them to call with their decision on the Monday or Tuesday, once they have reflected fully. Experience suggests that most candidates will go on to accept the job, but a minority will recognise that they are not suited to the role at this stage.

Once the analyst has been hired, they will need to be thoroughly trained. The training period will depend on the complexity of local law, but as a general rule of thumb it should start with the analyst spending 1 – 2 weeks working with law enforcement to see how they look at images, what information they collect and how they make decisions about the legal status of content, etc. It may also be appropriate to receive some training from industry (e.g. on how different technologies can be used) during this time.

After this initial period, the analyst should begin responding to reports coming in through the hotline. For the first few weeks, the analyst should either look at all reports together with an experienced law enforcement officer or send the URL and their initial assessment to the officer for his appraisal. As the analyst's skills and confidence grow, this process can be phased out and the analyst can begin to work more independently.

Naturally, the analyst should continue to liaise closely with law enforcement colleagues – not just during the training period – particularly for consultations on 'borderline' images (i.e. where it is not a clear decision whether the image is illegal or not). Consider involving your local LE contact in the recruitment process: this is partly to take advantage or his / her experience and judgement, partly to ensure that (s)he will be able to work successfully with your preferred candidate, and finally, so that he can take them through the final stage of the interview process which will involve them looking at real examples of illegal content.

By six months, the analyst should be analysing images competently. If, after this probation period, they are still failing to reach the right decisions and gather the correct information, then they are probably not the right person for the job and an alternative should be sought.

Close contact and ongoing monitoring by law enforcement will enable the analyst's judgement to be tracked; analysts will also need to keep abreast of changes to legislation and changing attitudes / interpretations of existing legislation (although the communications manager may also be able to take primary responsibility for the latter – see below).

Communications manager

The communications manager is the 'corporate face' of the hotline. This person's role is to promote the work of the hotline and raise awareness of its existence and role, as well as building and maintaining a strong working relationship with industry generally and key service providers in particular.

The individual will need to be a strong communicator and feel comfortable dealing with a range of external stakeholders including government and regulatory representatives. They will need to have a good grasp of related policy and legislative issues, although will not need to be trained in content analysis.

This person is also likely to manage the administrative aspects of the hotline – for example, managing funding processes, developing policies, keeping abreast of changes to legislation or changing standards / interpretations of existing legislation.

This person may also need to represent the organisation in international meetings and capacity building workshops, sharing good practices and emerging challenges. By constantly engaging with relevant stakeholders it is possible to keep abreast of the latest international developments.

4.2.2 Case study: Extracts from a content analyst job description, IWF (UK)

Note: The job description below illustrates the qualities required by analysts at an established "high-end" hotline with strong existing ties with law enforcement and so on. It is a useful guide, but bear in mind that not all the duties outlined will be relevant to new hotlines or hotlines in other countries.

Duties

- Processing reports from the public, IT professionals and other sources through the IWF's Report Management System
- Locate internet content e.g. websites, online groups or Usenet new articles. Analyse the content and assess whether it is potentially illegal under UK law, particularly images of child sexual abuse or criminally obscene content hosted in the UK and incitement to racial hatred material hosted in the UK
- Accurately trace the content's geographical origins
- Collate necessary evidence if assessed as potentially illegal under UK law
- Format a notification of the online content and its origins. Send this to the UK's Child Exploitation and Online Protection Centre. Also disseminate to the other UK police units, UK Internet Service Providers (ISPs) and international hotlines as relevant (see International Association of Internet Hotlines[16]
- Produce detailed reports of current trends in relation to potentially illegal content to help stakeholders to develop strategies to combat such material. Provide presentations when required.
- Liaise with UK ISPs, specialist police units, international hotlines, etc. as necessary
- Provide feedback to reporters
- Proactively monitor Usenet newsgroups/web for potentially illegal images as directed
- Deal with reports regarding the internet, which fall outside the IWF's core remit

Skills and abilities – Essential

- Demonstrates a high degree of accuracy and attention to detail
- Demonstrates a systematic and methodical approach to work
- Proven ability to see tasks through to the end
- Proven ability to communicate effectively in writing and verbally in a clear, concise and open manner
- Proven ability to use spreadsheets and produce reports and graphics from them
- Proven ability to distribute information efficiently, accurately and in a timely manner
- Demonstrates excellent IT skills, particularly using the Internet, including operating email client and web browser
- Demonstrates an ability to learn new IT skills quickly

Skills and abilities – Desirable

- Experience of using MS Outlook or Outlook Express
- Evidences a knowledge of a variety of internet browsers such as Firefox
- Demonstrates a good knowledge and understanding of the engineering of the internet and its technologies e.g. TCP/IP, http, html
- Relevant experience of producing research papers

Experience – Essential

- Experience of using and manipulating a variety of databases
- Understands the principle of confidentiality and evidence of having operated in an environment of confidentiality

Experience – Desirable

- Experience of working in partnership with external agencies
- Knowledge and understanding of the Data Protection Act
- Up to date knowledge of legislation and current events relevant to the IWF remit
- Basic understanding of police infrastructure
- Experience of presenting statistics to an audience

Personal qualities – Essential

- Proven ability to work as part of a small dedicated team
- Demonstrates a flexible approach to work
- Demonstrates empathy and concern for others
- Evidence of ability to encourage others to express themselves openly
- Demonstrates a range of mechanisms for dealing with stress and can recognise when to use them
- Shows respect for others' feelings, views and circumstances
- Accepts responsibility and accountability for own work
- Seeks and uses professional support appropriately
- Shows a realistic appreciation of the challenges of working within this environment

4.2.3 Team support and safety

Legal support

It is critical to ensure that employees have the necessary permission to do their jobs – e.g. written confirmation from government and / or law enforcement that they are allowed to look at and process illegal content.

Physical safety

Minimise contact with people who have made reports. If the hotline website has a large and expansive FAQ (Frequently Asked Questions) section, it should be possible to direct the reporter to this section once they have filed their report with a note saying "we have received your report and this is how it will be handled…" (then outline the process for reviewing the content, and what happens next, etc). This would avoid entering into a dialogue.

Where there is to be contact (e.g. to inform the reporter of the decision relating to the content they reported), try to use email as a general rule – it is a reasonable assumption that if someone has access to the internet they will also have access to an email account. If analysts do enter into email contact with reporters, they should not give out real names but sign off using only their initials.

If there is a perceived need to offer the option to report by phone, use an answer phone with a message saying "Please leave the URL you would like to report. Unfortunately we are not able to call you back" – do not have a telephone relationship with people reporting content.

Psychological support

The environment in which content is analysed is important and should be as relaxed as possible – analysts should be encouraged to discuss what they are looking at and feel free to talk about anything, they should be given the opportunity to have the radio on, go for breaks or go outside for a cigarette etc, as necessary. Of particular importance is that the analyst must never be alone in a room looking at images of child sexual abuse and other traumatic content. Even if the analyst is not sharing the image or showing it to the other person, it is extremely valuable to be able to express one's shock to another person in the room and have their support and empathy should the need arise, or simply to have someone else there to create an atmosphere of normality whilst witnessing images of events and situations that are potentially horrifying.

If the hotline has a team of analysts, the problem should not arise. If (as in the model outlined above) there is only one analyst and one other employee, the analyst should use information provided by the report (e.g. URL plus description of type of content) to plan his workload so that he has a reasonable expectation of looking at non-traumatic content (e.g. written word extreme right / racist content is unlikely to traumatize the vast majority of people even if it is potentially illegal) if he is working alone for a period of time.

Colleagues should be encouraged to be aware of each other's behaviour and changes in behaviour – for example, an analyst who is working more slowly than others and / or taking longer breaks and / or not taking part in general office chatter and humour, may be feeling traumatised by or stressed about their work.

In terms of formal support from a psychology professional, employees should have a regular meeting with their counsellor every three months. Support should also be available at any time, should the analyst feel the need for contact between scheduled appointments.

When advertising for a support counsellor for the hotline, it is worth considering involving the staff in the recruitment process and allowing them to choose the person themselves – it is critical that the staff can trust and communicate comfortably with the appointed counsellor. Potentially suitable counsellors could include those who have previous experience of working with policemen, fire fighters, emergency response teams (air crash, traffic incidents etc), and so on.

Meldpunt (Netherlands) observes the following guiding principles to support the welfare of its staff:

- Nobody works alone in the office, as far as possible.
- Everyone works on reports together in morning. So half the day is spent on reports, and half the day on other tasks.
- All colleagues work full days. This way everyone spends an equal amount of time on reports.
- All employees deal with reports so no one feels excluded.

Further reading

Members of INHOPE will be provided with a specific Welfare document providing details on the full range of issues to be managed with regards to staff welfare.

Chapter 5
Operations

This section contains general principles as well as working examples of how hotlines manage processes and practicalities within their day to day operations.

5.1 Online reporting forms

The main aim of the online reporting form is to capture the URL. However, if there are additional steps in the reporting form beyond this, there is the potential to gather more useful information. For example, if the person reporting the URL also flags the nature (e.g. racist / extreme adult / child sexual abuse) and type (e.g. written word / image) of content they believe they are reporting, that can help the analyst prioritise their workload or minimise the risk of looking at traumatic content when they are alone (see *Psychological Support / Team Support*, above).

If the form asks for too much information, there is a risk that the reporter may not complete the process - although experience suggests that this tends not to be the case and that once someone has taken the decision to report they tend to be committed and follow through to the end. A useful approach is therefore to order the questions by priority – always starting with the URL – and to submit each piece of information as it is entered, so that if a reporter aborts without finishing the process, the information which has already been entered is not lost.

5.2 Managing reports of illegal content from internet users

Hotlines should explain clearly how reports will be managed. For example, INHOPE requires members to communicate how reports will be handled, along the following lines: "We will assess your report according to the law in our country and if is illegal the location of the reported material will be passed to the police and if it is overseas we will forward it to the relevant INHOPE hotline".

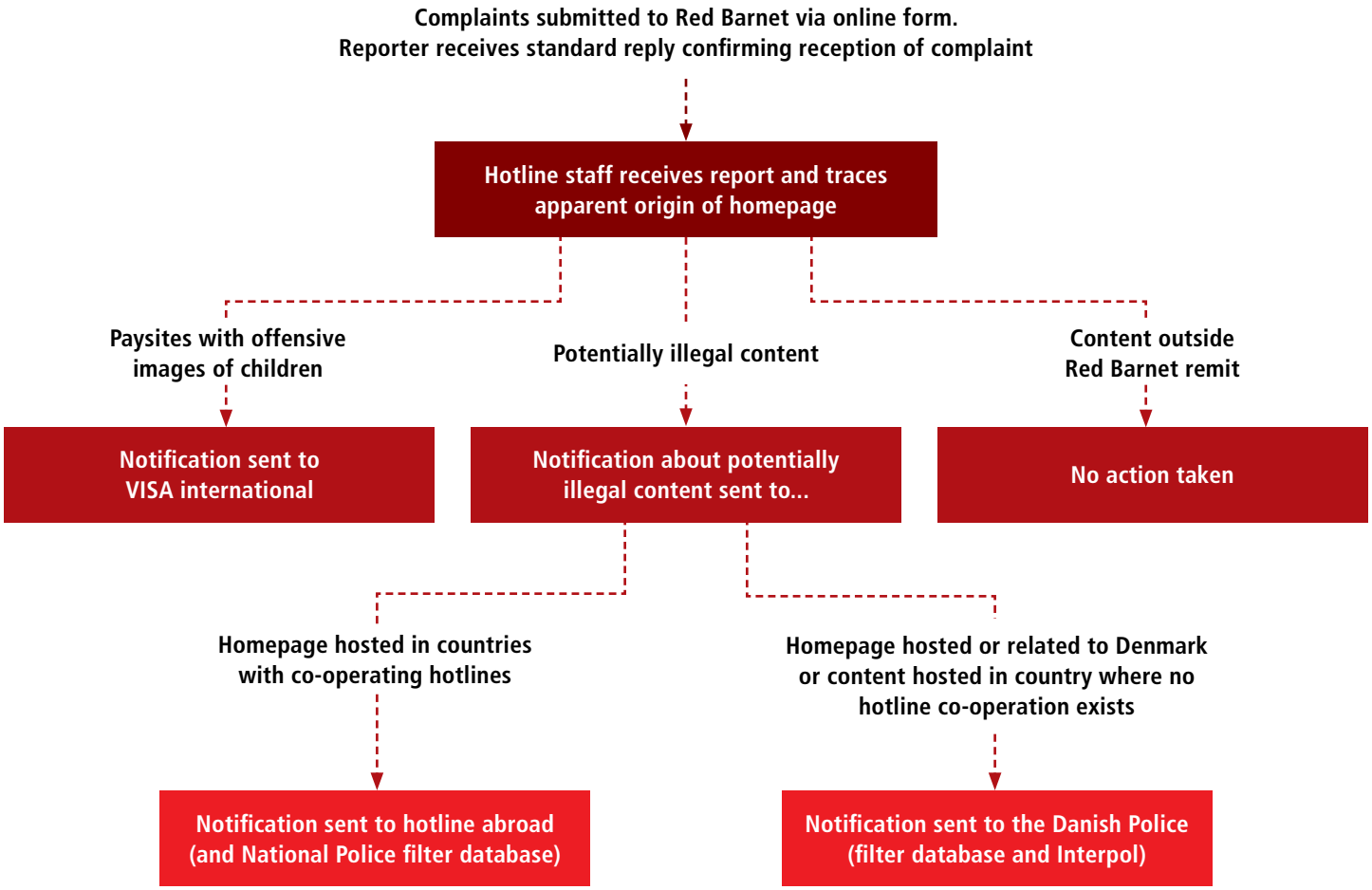
In general terms, a report will be handled along the following lines:

- A report is received by the hotline.
- The hotline's analysts will look at their own hotline database to see whether the content in question has already been reported and is in the system.
- If the content has not previously been reported, it will then be assessed for illegality in that particular country.
- If content is found to be illegal under national legislation and hosted in that same country, national processes will commence – in some countries, for example, the relevant ISP will be contacted immediately by the hotline directly and NTD processes will be instigated, in others, the report will go to law enforcement in the first instance.
- If it is found to be illegal under national legislation and hosted in another country, then the information will be cross-checked against the central INHOPE database to see if it has already been reported by another hotline. If the URL and details are found to match something already in the database, then there is no need to report it again centrally. But for the hotline's for own records, they can note that they have received a report and that the URL in question is being dealt with by the relevant country / hotline / law enforcement agency / etc. It is also possible to go into central database at a later date to see the status of the content (e.g. content was reported on 7 May by hotline X, removed on 9 May by host in country Y).

However, each hotline and market will have its own specific process that will depend on factors such as the national legislation and the nature of working relations with national law enforcement.

Where possible, it is best practice for hotlines to notify the national LEA of confirmed instances of illegal content being discovered – however, in practice, this will depend on each country's law enforcement practices.

Case study: Red Barnet (Save the Children Denmark)



5.3 Managing reports of illegal content from industry

The overall process for managing reports of illegal content from industry will be broadly the same as managing reports which have come directly to the hotline from the 'end user'[17].

However, as the report will be passed on from industry, rather than coming directly from the source, the hotline will have to work from whatever information is given about the content – which may just be a URL with no additional description, for example. Industry partners should be encouraged to collect, where possible, the same types of information from the reporter as the hotline would have done had the report come directly to them (see section on online reporting forms, above).

The key thing to communicate to industry partners is that any report they receive of content that is potentially illegal (not copyright issues, but psychologically damaging material such as child abuse content or extreme violent / sexual content) that they receive from a user, should be passed straight on to the hotline for review. For example, if the reporter has sent through a file of images, these should be forwarded straight the hotline without being opened. This will spare industry staff the trauma of viewing illegal and extreme content.

The hotline should revert to the industry partner with its findings, which the industry partner can communicate onwards to the original reporter. If the findings are that illegal content is being hosted on the partner's services, then that company's Notice and Take Down processes may also commence at that time (depending on national legislation / law enforcement requirements).

The hotline does not need to know the reporter's name or details – industry partners can communicate to their users that reports will be passed on to the hotline directly by the partner company without the individual's details, and that they will be given the outcome of the report by the partner company once it hears back from the hotline. This gives users a sense of extra security if they are concerned about making a report directly to a hotline.

5.4 Analysing findings and trends, and using this information

Many well-established hotlines, such as the UK's IWF, are now able to provide detailed analyses of trends in online child sexual abuse content – where content is hosted, how severe the abuse is, the apparent age of the children in the images, and so on.

This type of information is valuable in informing the message when trying to educate groups or organisations as to the nature and extent of the problem of online child sexual abuse content. It can also help stakeholders to understand changes in behaviour which can support investigative processes and the development of deterrents (an example of this might be the introduction blocking access to URLs which are known to contain illegal content hosted in other countries where processes to remove the content are less rigorous).

A new hotline should not expect to generate similar levels of information. If statistics are needed for the hotline's own education purposes, use those generated by e.g. INHOPE, the IWF or NCMEC.

For reporting purposes in the early years, hotlines should seek – primarily for their own records – to focus on how many reports were received, what proportion of these were found to be illegal upon examination, how many reports were passed to law enforcement, how many resulted in NTD procedures being instigated in that market, and so on.

By contributing to the centralised INHOPE database, hotlines will automatically be helping to generate some data. And as the hotline's operation grows, they should aim to begin reporting in greater detail – all information is useful from a law enforcement perspective: providing information on trends such as 'key words' to search on, or series of websites using a particular name moving between ISPs, can all support police investigations.

17 Note: in some countries existing agreements / legislation will mean that industry reports are made directly to law enforcement, in which case this section will not apply.

5.5 Availability

Hotlines typically work on a Monday – Friday, 9 – 5 basis. They are almost always dealing with something static (an image that has been posted, for example) so there is no immediate urgency. Options for "what to do if your report relates to a child being in immediate and current danger" should be shown on the website / reporting page – e.g. a number on which to call the national police, a link to the Virtual Global Taskforce, etc.

Chapter 6
Communication

Awareness of the hotline is critical to its success, as is its credibility – if people do not know there is a hotline, they cannot report illegal content if they find it; if they do not trust the hotline, they will not report illegal content if they find it.

As such, communication will play a key part in the hotline's ability to achieve its goals.

6.1 Messaging

Headline messaging for the hotline will be shaped by the hotline's defined scope and remit, but it must be simple, clear, and memorable. Headline messaging must resonate with all stakeholders and it must communicate that the hotline:

- Is entirely focused on illegal content (ideally only child sexual abuse content, depending on whether this can be negotiated with government, etc).
- Has independence, and is firmly committed to its defined scope (as above) – and therefore is not and will not be involved in removing other types of content (e.g. it will not be censoring content which is perceived by some to be 'unsuitable', it will not be involved in politics or curbing freedom of speech). This kind of transparency is critical to the hotline's reputation and to ongoing trust in the hotline and its processes.
- Is part of – and works in partnership with – a wider, international effort to combat illegal online [child sexual abuse] content; is a member of INHOPE.
- Has the support of government, law enforcement, industry and NGOs, and the international community (the latter may be of particular importance in countries which do not have high levels of trust in their national government and / or LEA).
- Does not hold data on / prosecute / etc anyone who reports content.

Additional messages on the hotline's website can be more detailed, but the aim must always be to make the hotline's operations and objectives as clear as possible. Information to include on the hotline's website should include:

- What happens when a report is made? (NTD, INHOPE database, Interpol, etc).
- Does the reporter have the right to be told the outcome of the findings?
- Can reports be made anonymously?
- Who is involved in the decision making process and what are the escalation processes if there is no clear answer?
- What is the governance structure? Who holds the hotline accountable?
- How is the hotline funded?

The hotline should also build up a directory (perhaps as a sub-section of the FAQ section) with information which redirects people who are reporting issues which fall outside of the hotline's remit – these reports are likely to wide-ranging and include areas as diverse as online purchases which have been paid for but were never delivered, and concerns about specific children at risk of abuse in real-time. Be as inclusive and specific as possible, and offer contact details for all relevant companies, organisations, official bodies, NGOs, and so on: for example, "If you have been a victim of fraud on the internet, contact XYZ; if you want to make a report about a child who is currently in danger of being abused, contact ABC".

In a similar way, encourage relevant official bodies, NGOs, industry partners and so on, to use their websites to direct people wishing to report illegal online content to the hotline website.

6.2 Awareness-raising

Awareness-raising campaigns will be critical at launch, but will also be an ongoing part of hotline operations. This will include generating national press coverage, as well as working in more targeted ways – for example, trying to reach out to corporate IT managers through industry press or training programmes.

Public awareness can be dramatically increased by press coverage, in particular at the time of launching the hotline. Also use the internet and the promotional power of your partners. Have the following in place for the hotline's formal launch:

- Headline messaging (as in 6.1, above) that has been agreed by all key stakeholders.
- A press release with quotes from key stakeholders and opinion formers, for example: a minister, a law enforcement officer, NGOs and industry. The aim is to show collaboration and support, so that people will feel comfortable reporting.
- Have links to the hotline website from the state / government website, the LEA website, and as many industry partners as possible.

If possible, try to hold a launch event / conference with speakers from the different stakeholder groups to show a united front and, potentially, generate TV coverage. Also try to think creatively about using what is available through your partners – does a mobile operator partner have subscribers who accept promotional SMS messages, for example?

Use the hotline's relationship with law enforcement to help get the message out. For example, the national LEA's website could carry a message stating that if users are looking to report illegal content they should contact the hotline directly. Similarly, from a media perspective, if law enforcement representatives are being interviewed about issues related to those managed by the hotline, they can use this as an opportunity to advocate the hotline and its role.

The hotline's first year of operations will largely be spent getting the message out – take opportunities to present about the hotline and its activities at conferences and events, communicate about success stories (e.g. the hotline passed on a report to police which resulted in the arrest of X people in country Y) and learn from other hotlines who have developed a range of means to encourage reporting (see case study below).

Case study: Software plug-ins, New Zealand

Software plug-ins, such as those offered by hotlines including the New Zealand Child Alert Hotline (http://www.ecpat.org.nz/Make-a-Report/Child-Alert-Hotline/Download-Child-ALERT-Hotline.aspx), help users to report a site automatically by filling the necessary fields (URLs, date / Time accessed etc) and opening the relevant hotline page without having to search for a suitable hotline. The user downloads the plug-in, which then appears on the toolbar, and if the user stumbles upon a website they believe to contain illegal content, they simply click the button and the plug-in automatically captures all the necessary information and passes it on to the hotline.

Plug-ins could be distributed to the public by working in collaboration with partner ISPs, as well as being offered through the hotline website itself.

Chapter 7
Additional options for emerging markets

Smaller countries or countries with lower level of internet penetration may wish to consider working with the INHOPE Foundation or IWF International.

7.1 INHOPE Foundation

Historically, because much of the funding for INHOPE and the European hotlines comes from the European Commission, the INHOPE Association focused primarily on identifying and assisting with the development of hotlines within Europe.

However, the INHOPE Association is now using the experience it has built up developing hotlines in Europe to help develop hotlines globally.

Some of the European hotlines and some of the larger-sized non-European hotlines are self-funded or have the financial support from industry and governments to run their operations. However, in many emerging countries there is a lack of funding, interest, or even legislation in this area. INHOPE found that the problem of child exploitation is often not addressed, much less reported to law enforcement agencies. The success of the INHOPE model is based on the notion that the public would report child exploitation to non-governmental bodies if they could do so anonymously and that their reports would be considered by a professional organisation that is trusted to refer appropriate illegal content to the right body, whether that be a statutory body or simply the internet service provider whose services had been compromised. Many non-governmental organisations try to address this issue, but lack the financial resources, expertise, and best practices knowledge.

To help address this, the INHOPE Foundation was created to support the development of hotlines in areas of greatest need. The INHOPE Foundation has five primary objectives in order to enhance international cooperation to eliminate illegal content, especially child sexual abuse material, from the internet and other online communication services. Those five primary objectives are:

1 To raise funds to use in the development of new hotlines worldwide

2 To financially sponsor and support start-up activities of participants of the foundation in the development of new hotlines to enable a controlled expansion of the INHOPE network, prioritizing countries where child sexual abuse material is being facilitated, or distributed, online

3 To utilize funding for the purpose of identifying potential participants

4 To develop regional training, coordination and implementation of best practices and standardization of reporting and analysis for participants

5 To continue development support and education for participants and to advise participants in the creation and operation of a hotline.

The INHOPE Foundation can provide initial 'start-up' support and training on best practices to the staff of qualified organisations within specifically targeted countries to develop a hotline that addresses the issue of child sexual victimisation via the internet. The Foundation also provides guided oversight during the initial start-up phase, including instruction on best practices for staffing requirements, equipment needs, location security, data safeguarding, and internal and external policy development. INHOPE Foundation staff can also work with the local organisation to report on the development of the new hotline within an agreed time frame.

Through a generous grant agreement from the Oak Foundation, the INHOPE Foundation is aiming to help create and / or enhance 9-12 new hotlines outside of Europe over the next three years.

7.2 IWF International

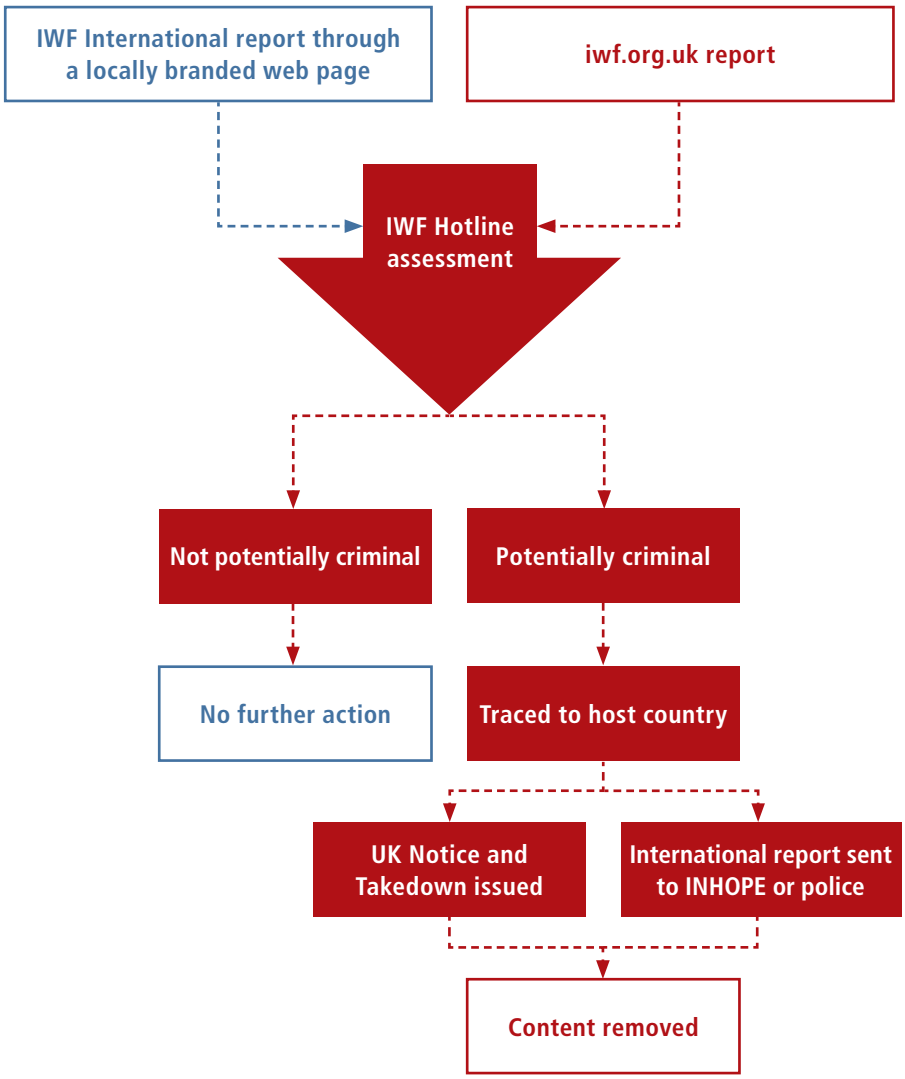
In January 2013, the UK's hotline, the Internet Watch Foundation, began offering its services to other countries with no national hotline, in particular those countries which are expanding their digital infrastructure and experiencing a rise in the level of internet use amongst their population.

Under the 'IWF International' model, IWF first provides a countrywide assessment of the local need for the service, and then produces a report and implementation plan. As part of this process, IWF carries out an assessment of local legislation to ensure parity, where possible, based upon relevant UK Law or Commonwealth Law.

Each country has its own locally-branded reporting page where citizens can report online child sexual abuse content. When a report is made, it is sent to the IWF in the UK who assess the content within 24 hours and take the appropriate action, including tracing where the content is hosted, alerting the host country to the content, issuing notices to get it removed (Notice and Takedown) and informing law enforcement. A progress report is sent to the partner organisation in the country where the report was made, and the country only pays for each report that is processed with no additional overheads.

Countries working with IWF International will also have access to the IWF List to block and filter child sexual abuse content, as well as use of the IWF Keyword List.

A simple flow diagram to show how child sexual abuse content will be assessed and removed through IWF International



Chapter 8
Contacts

Contributing to this document and requests for further information:

If your organisation has experience in this area and is in a position to contribute to the evolution of this document, or if you require any additional information, please contact: Natasha Jackson, njackson@gsma.com

Contacting organisations listed in this document:

If you wish to contact INHOPE or the INHOPE Foundation, please email: secretariat@inhope.org

If you wish to contact IWF International, please email: fred@iwf.org.uk

For enquiries relating to ICMEC's training programmes, please email: Guillermo Galarza (Program Director, Training Programs and Outreach) ggalarza@icmec.org

If you wish to contact Interpol, please email Natasha Jackson, njackson@gsma.com at the GSMA in the first instance

Chapter 9
Acknowledgements

This toolkit was developed by the GSMA in collaboration with INHOPE, with support from a number of organisations who play a key role in the fight against online child sexual abuse content. The document incorporates information contributed by the following individuals and organisations, who generously shared their experiences and expertise:

Russell Chadwick – INHOPE
Peter Robbins – INHOPE
Dieter Carstensen – Save the Children, Denmark
Anjan Bose – ECPAT International
Agnese Krike – Net Safe Latvia
Mick Moran – Interpol
Guillermo Galarza – ICMEC
Maaike Pekelharing – Meldpunt Kinderporno op internet
María José Cantarino de Frías – Telefonica
Emma Lowther – IWF
Fred Langford – IWF
Susie Hargreaves – IWF

GSMA Head Office
Seventh Floor, 5 New Street Square, New Fetter Lane
London, EC4A 3BF, United Kingdom
Tel: +44 (0)207 356 0600

http://www.gsma.com/myouth