# Logistics

Once the legal, political and operational framework of a new hotline is agreed upon by all national stakeholders, the logistics of hotline development, including hardware, software and physical location are relatively straight-forward.

A common question and concern for new initiatives relates to the 'cost' and 'resource burden' of setting up a hotline.

In reality, the resources need to set up and run a hotline will depend on:
1. The resources that are already available for the hotline project
2. Local costs in the country of operation

A common and cost-effective solution is to establish the hotline as a new service within an existing organisation. This will help to control the costs of office space, equipment and staff.

OFFICE SPACE

HARDWARE, SOFTWARE AND INTERNET CONNECTION

TRAINED STAFF
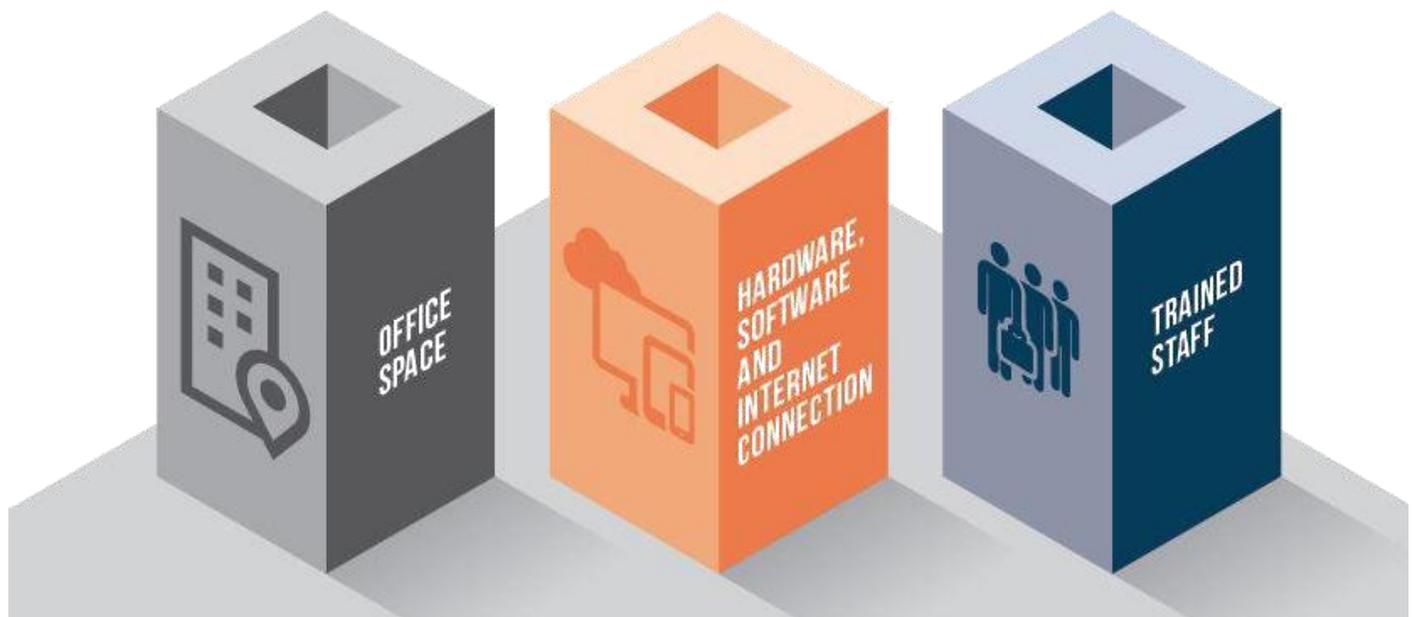
PDF download: infographic-2016_basic-building-blocks
(http://hotlinedevelopmentguide.org/cms/wp-content/uploads/2016/12/Infographic-2016_Basic-Building-Blocks.pdf)

Technical infrastructure of the hotline

A snapshot of the existing network of hotlines demonstrates that there is no single model of hotline.
They represent diversity of size, sector and coverage.
Hardware

For start-up initiatives, the basic requirements for hardware include:

- Computer with internet access, ideally using a dedicated fixed IP address
- Server for the website used to receive reports from the public
- Separate server or computer for the local Report Management System (RMS)

Software

Report Management System

Regardless of the size of the hotline or the volume of reports, a hotline needs to implement a database or Report Management System (RMS) for tracking and handling reports. The RMS will vary in size and complexity according to the hotline.

An RMS can be created using:

1. Standard software such as MS Access

2. Bespoke software already in use and transferable from another hotline, or developed for the new hotline

The RMS may allow for reports to be referred directly to law enforcement and industry partners, or even provide these partners with direct access to reports marked for their attention in a secure environment.

If reports will be referred manually and outside the secure environment of the RMS, careful consideration must be given to how this happens. Confidential information for law enforcement or an ISP should be shared in a secure way. One option is to send encrypted information via email.

Security

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. 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"network14 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.

INHOPE – International Report Management System ICCAM

For INHOPE members, INHOPE provides access to an international RMS / technology platform 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.

Additionally, INHOPE's systems provide content matching capabilities that identifies previously seen images and videos and makes relevant information available to INTERPOL.
INTERPOL actively cooperates with the INHOPE platform by downloading the hotline- reported CSAM daily.

Previously unknown images are uploaded by INTERPOL into the ICSE database with the aim of identifying victims and referring cases to appropriate national law enforcement. Currently, 48 INTERPOL member states and EUROPOL are connected to the ICSE database and they collectively work to identify victims. Cases are shared through the INTERPOL secure network to the non-ICSE database connected countries when necessary. There are more countries to be connected in the next 4 years.

Investigation tools

INHOPE offers training for members and new hotlines on a range of topics relevant to the management of reports. This includes 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
- Visualroute – 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.

Office set-up and controlled access

The workstation 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.

Hotline Staff

The introduction of a hotline for the assessment of reports of online child sexual abuse material has implications for the parent organisation.
Close attention must be paid to:

1. The specific legal issues concerning the management of child sexual abuse material in its country of operation

2. The technological dimensions of content distribution and storage
3. The crucial nature of international cooperation and timely report referral

4. The sensitive nature of the subject matter

5. The selection, training and support of staff who will process reports

The learning curve of the hotline in each of these areas will depend on the nature of the parent organisation. For example, if the organisation and staff have experience dealing with the sexual exploitation and abuse of children, which may include previous exposure to child sexual abuse material, it may be that more attention will be paid to technical and issues at the start.

If the parent organisation is operated by an industry or government body, closer attention may be paid at the start to the recruitment and training of staff to deal with child sexual abuse material, and there may be a higher starting level of technical and legal knowledge.

Whatever the case, building a strong and capable team is one of the most important aspects of setting up the hotline.

INHOPE in action

"Child sexual abuse: the people who watch it to remove it", a newspaper once ran as a headline. Our network's analysts take great pride in their work. **They act as first responders in the online safety ecosystem** and therefore **help build trust and resilience.** It is skilled, difficult and often very challenging work, which not many people can consistently do - that is what makes them so special – they are the "Unsung Heroes".

Our People

No crime is as borderless as cybercrime, yet the **jurisdictional focus remains national** in nature. The content is traced back by analysts to the country of hosting. In other words, the laws where the servers are located are applicable.

The INHOPE network connects 51 hotlines and 170 expert analysts around the globe, who operate within INHOPE best practices and use common technical tools. Our network's analysts are devoted, hyper-connected and talented individuals who determine if the content fails legal tests and who harness the power of technology for the greater good.

Analysts assess the reports of suspected CSAM in a consistent, professional, objective and systematic way so that content is categorised, information collected, notifications to industry tracked, access to content removed, validated information

forwarded to law enforcement so hopefully perpetrators can be brought to justice and victims can be identified and rescued.

INHOPE member hotlines alert industry partners when their platforms are being misused for criminal activities pertaining to the distribution of CSAM and therefore help deliver Corporate Social Responsibility (CSR) of the ICT sector.

REPORT ILLEGAL CONTENT

Faster, Better, Stronger **Together**

www.inhope.org

Team: structure, recruiting and training

The number of staff needed to operate a hotline will depend upon several elements:

1. The expected or existing volume of reports to the hotline. For example, an organisation may decide to implement a hotline in response to unsolicited reports of online CSEA from the public, in which case initial estimates of volume can be made. However, if a hotline is established as an evidence-based response to online CSEA, it will not always be easy to predict how quickly and at what volume reports will be sent to the hotline. Whichever the case, it is advisable to start small.

2. The initial team should consist of:
   ○ The equivalent of one content analyst – two trained analysts working on reports as part of their overall activities

○ One hotline manager who may carry out report analysis but is also responsible for overseeing the policy, operations and possibly also the communications of the hotline service.

3. The arrangements in place to hire staff for the hotline. Depending on the funding and existing infrastructure available for the hotline, the organisation may be required to launch the hotline with staff already in place. If this is the case, specific training and support must be provided to hotline analysts, even if they are experienced in the issues, and consideration must be given to guidelines on the welfare of hotline staff

Content analyst(s)

The volume of reports handled by existing hotlines in the INHOPE network is very varied. In the region of 1000 reports in the first year of operation would be considered a promising start.

For a start-up hotline, it is unlikely that the content analyst will be required to spend 100% of his or her time on reports. A typical content analyst will be able to deal comfortably with 100 reports a week which means that only one content analyst will be required to get the hotline facility up and running.

The organisation running the hotline will need to monitor the workload of hotline staff and make a decision about additional staff according to resources available. However, in a fully-functioning hotline, 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.

Attention to report management time is also important for the rapid removal of child sexual abuse material at source. This may mean referral to law enforcement and/or an Electronic Service Provider in the hotline of the country, or referral to a hotline in another country. Quality and speed of report management are essential to the success of a hotline.

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

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. From a psychological wellness perspective, the organisation should ensure that the content analyst has responsibilities within their workload not related to the content analysis, whether administrative or other.

Selection

In general, a content analyst should have the following experience:

Technical

Ideally, a basic interest in and understanding of how websites and content distribution over the Internet works and the fundamentals of online security / personal security on the web. However, they do not need to be a technical expert. INHOPE can provide access to online training for orientation in this area.

Legal

Able to assimilate and apply the relevant legislation of the country and the specific guidelines laid out for the hotline for classifying content and managing reports. The person should also be comfortable presenting to stakeholders such as law enforcement. This will include the ability to describe and discuss graphic content in a factual and pragmatic tone.

Subject-matter

Experience with some aspect of combatting child sexual exploitation is not essential but can be very beneficial to the ability of the analyst to interpret the work of the hotline in its wider context. For example, a person with experience dealing with child victims and working with the national government to prevent and respond to child sexual exploitation and abuse is in a good position to 'transition' towards a focus on these issues in the online context. In this case, training in the technical aspects of content distribution over the Internet and in the management of reports can be provided to support that transition.
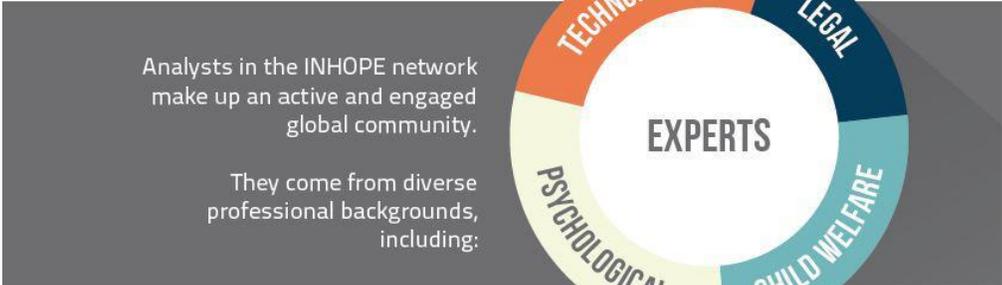
Personal

In addition to any specific knowledge of the topic, the person should have some life experience and maturity. Experience shows that new graduate recruits have been shown to have higher turnover than more mature recruits.

However, avoid making 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.

Hotlines: Diversity of people

INHOPE Foundation

Analysts working in hotlines around the world take great pride in their work. They act as first responders in the online safety ecosystem. They do skilled, difficult and often very challenging work and they show great resilience.

Analysts in the INHOPE network make up an active and engaged global community.

They come from diverse professional backgrounds, including:

EXPERTS

TECHNOLOGICAL

LEGAL

CHILD WELFARE

PSYCHOLOGICAL

Interviews

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.

The final stage of recruitment should also be used to give the candidate the opportunity to find out for him or herself whether or not they are temperamentally suited to the role. Even if the candidate has experience working on the topic, it is important for him/her to consider the specific nature and demands of content analysis.

Once the preferred candidate for the role has been selected, all available police and background checks should be carried out.

Depending on the employment laws in the country of operation, the organisation can consider giving the candidate a 'temporary' contract acknowledging that they understand the nature of the content they will be viewing and assessing.

After an offer is made, 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 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 pay attention to and 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.

In the case of new hotlines, a visit to the specialised law enforcement unit, or to an experienced hotline after recruitment of at least one analyst can substitute this internal process.

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.

Indeed, deciding to work as a content analyst is a decision that must be made willingly. Even if the organisation offers the candidate a short period of reflection, there are cases where a new content analyst decides after several weeks or months of work that they do not wish to continue. It is important that the employer provides a non-judgmental environment and where possible, can offer the employee alternative work within the organisation.

Training

Once the analyst has been hired, they will need to be thoroughly trained. The training period will depend on the complexity of local law and the technical knowledge of the analyst.

In the case of new hotlines, the analyst will often be learning and developing along with the hotline service itself. This reality emphasises the need for close cooperation with law enforcement and industry partners from the start so that mistakes can be addressed as part of the learning process. In the beginning, quality of assessment should be prioritized over speed of assessment, particularly because accurate content assessment by a hotline is fundamental to its ability to build trust with the public and key stakeholders, and to cooperate effectively with the international network of hotlines.

The following options are possible for training at the start and throughout the life of the hotline:

- **Training by the local specialised law enforcement unit** – ideally this will happen in the first few weeks and will continue on as regular a basis as possible.

After initial training by law enforcement, 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, and the law enforcement unit sees the accuracy and value of the hotline's work, 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).

- **Joint hotline and law enforcement training by an international law enforcement partner**
  or affiliated partner – this should not substitute but will certainly complement local training. It is also a very useful way to build an international network for the hotline.
- **Training by an experienced hotline analyst in an existing hotline within the INHOPE network** – peer-led training will help orient the new analyst in his/her work, and experienced analysts are best placed to answer questions and solve issues that are specific to hotline work.
- **Training by INHOPE** – INHOPE offers a range of online and face to face training for its members, but can also devise a programme of training for staff at new hotlines.
- **Training by a local or international Industry partner** – this form of training will not only help the hotline analyst understand the perspective of Industry and the way different technologies are used to exploit children, but it will also help the hotline build its relationship with its Industry partners as key allies in its work.

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.

In many cases, the hotline service will be part of a wider range of activities carried out by the parent organisation. In this case, existing communications capacity and experience should be applied to the promotion of the hotline. This will likely require some training, and the hotline will benefit from interaction with experienced hotlines.

For the video, please visit http://hotlinedevelopmentguide.org/guide/logistics/

Team support and safety

Legal support

It is critical to ensure that employees have the necessary permission to do their jobs, and that they and the parent organisation has protection when carrying out the activities of the hotline.

The nature of protection and authorisation needed will depend on several factors, in particular the specifics of the national legislation with regards the viewing, possession and storage of child sexual abuse material.
However, the hotline should seek written confirmation from government and / or law enforcement that they are allowed to look at and process illegal content. Ideally, a written agreement with the authorities will detail the role and mandate of the hotline.

Physical safety

Whether an Industry, civil society or governmental entity, the hotline's parent organisation will likely have existing security procedures in place that can be adapted to cover the specifics of the hotline's activities.
Some of the issues to consider include:

- The accessibility of the office to unexpected visitors and people with a potential interest in accessing the sensitive material processed by the hotline and/or the organisation
- The accessibility of the dedicated hotline space / room to unauthorised external and internal visitors
- The ability of people making reports about online child sexual abuse material, or people wanting to complain about an action taken the hotline in relation to these reports, to identify analysts.

Minimise contact with people who have made reports. Many will use the option to make an anonymous report and will not seek to engage further with the hotline. However, some reporters may wish to engage the hotline, request feedback or ask more general questions.

One way to minimise this engagement is to provide comprehensive information on the hotline's website, and to develop a Frequently Asked Questions (FAQ) section.

When designing the web-form, it will be possible to direct the reporter to this section once they have filed their report, or to send an automatic reply in the case that a report is submitted via email. The level of detail is up to the individual hotline, but to avoid further engagement, the reporter could be informed that:

- The hotline has received the report
- How the report will be processed
- What will be done with the report

If the hotline does offer feedback on request and therefore needs to make contact with the reporter, email is the best option. It is a reasonable assumption that if someone has access to the internet they will also have access to an email account.

However, when analysts do enter into email contact with reporters, they should send from a general account such as 'info@xxxx.com', and should not give out real names but sign off using only their initials or the name of the organisation.

If the hotline does provide a telephone reporting or general information service, identifiable personal contact should be avoided.

Given the format and length of many URL names, and the fact that reporters will come across URLs with CSAM when surfing the Internet, the use of the web-form should be preferable for most reporters and should be encouraged by the hotline on its website.

However, if a telephone service does exist, the hotline should use an answer phone service with a message such as: "Please leave the URL you would like to report. Unfortunately we are not able to call you back". The hotline should not have a telephone relationship with people reporting content.

Psychological support

The work of a content analyst will by its nature be impactful. However, the extent and nature of this impact can be reduced when an analyst understands the importance of his/her work and

feels supported by the hotline manager, colleagues and the parent organisation in general. Advice on support for hotline content analysts and staff includes:

- 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. Often the act of merely viewing a disturbing image with a colleague can help alleviate stress
- Analysts should feel free to talk about anything and even joke and chat with colleagues as a common way to alleviate stress when viewing content.
- They should be given the opportunity to have the radio on, go for breaks 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 a colleague, 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.

Simply having someone else in the room when viewing distressing content can help 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 because a peer-support structure should naturally take shape.

If, as in the model outlined above and common to new hotlines, there is only one analyst and one other employee, the analyst should factor this into his/her workload planning. If working alone for a longer period of time and on a regular basis, the analyst could:

- Use information provided by the report such as the URL plus the description of the type of content, to plan his/her workload and balance assessment of non-traumatic content with more traumatic content. For example, if the hotline accepts reports relating to issues other than child sexual abuse material, such as reports of the written word that may potentially be illegal under the local legislation (e.g. racism, xenophobia), they could focus on these reports for a period of time.
- Set aside a certain amount of time to deal with administrative or other tasks assigned to him/her that do not involve contact with any reports of online content.

Peer-support

Whatever the case, all colleagues of content analysts should be encouraged to pay attention to each other's behaviour and changes in that behaviour. Some indicators of heightened stress or trauma in an analyst could include:

- Slower work than other colleagues
- Taking longer breaks than previously
- Not taking part in general office chatter and humour

Formal support

Hotline staff should be required to speak with a psychology professional every three months. They should also have access to their counsellor between scheduled appointments on the basis of need. Any additional visits to the counsellor should be entirely confidential and access should be organised in a way that the analyst does not need permission from a line manager.

If the hotline does not have access to a psychologist and needs to identify a suitable candidate, 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 people exposed to traumatic situations such as policemen, firefighters and emergency response teams.

Even if the hotline employs a psychologist as one or more of its analysts, an independent psychologist will be important to encourage staff to discuss any issues affecting them.

For further guidance, see the INHOPE Best Practice Paper Staff Welfare 2013 (PDF) (http://hotlinedevelopmentguide.org/cms/wp-content/uploads/2016/04/Best-Practice-Staff-Welfare-2013.pdf).

Tips from hotlines in Sweden and Poland:

- Keep the hotline separated from other activities within the organisation. For example, have a separate room to which only hotline staff have access.
- Use a separate secure line for hotline internet access.
- Change the passwords and/or codes needed to access the hotline room/computer regularly. If possible, use both passwords and an electronic ID.
- If possible use two screens when working on the hotline. ECPAT Hotline uses one screen for the virtual computer, and one for ICCAM (INHOPE system)/e-mail/regular browser, etc. By doing this, you minimize the risk of opening a reported webpage outside of the virtual computer.
- Set the virtual computer to clear history when powered off, and establish a routine for updating the software (including plug-ins and software on the virtual computer).
- Keep the operating system of the hotline separated from the main office environment to protect the hotline's documents.
- Ensure the use of security certifications (https://) on the hotline website.

- Take steps to protect the privacy of content analysts – for example, avoid using personal signatures, profile in databases and email address in correspondence with reporters.

www.hotlinedevelopmentguide.org