7 Frequently Asked Questions (FAQs)

7.1 Quick Glance FAQs

1. **When do we get a 'buddy hotline' to support my organisation's development in setting up my hotline?**
   Around the same time as provisional membership starts (see timeline) or you can be put in touch earlier if required. INHOPE staff are always present to answer all your questions and support all your needs from the moment we are in touch with each other.

2. **When does my organisation become an active participant of ICCAM?**
   Once approved as a provisional member and once the ICCAM Participation Agreement is signed (all members must sign this document (for data protection purposes), you can participate in ICCAM.

3. **When do we get full member rights?**
   You can attend all training meetings and Annual General Meetings as long as your provisional (and later full) membership fees are paid. While many rights are granted to provisional members of INHOPE, during your first year as a provisional member of INHOPE, you do not have voting rights. This changes as soon as your application for full membership is granted by the full membership at a Hotline Training Meeting or Annual General Meeting.

4. **When do analysts undergo training?**
   If your organisation has opted to use Report Box, your first hotline training will be on Report Box in Months 1-4 of the timeline. Thereafter you will need to attend one of INHOPE's bi-annual Hotline Training Meetings where you will participate in a CORE training. The second training is a content assessment training provided by INTERPOL. Both trainings provide hotline analysts with the tools they need to trace content and understand in more depth how the internet works. CORE Training Meetings take place every six months for new analysts or analysts that require a refresher training. INHOPE also provides e-learning in several areas. Training is an ongoing process, and we organise focus groups and webinars throughout the year where we encourage your national law enforcement and industry to attend and participate in meetings with us and with you. For more information on INHOPE's trainings, check INHOPE's Training Policy.

5. **When do we receive public reports?**
   As soon as you have a web-reporting page in place you can receive reports. If you are using Report Box, then you need to still put a reporting form in place, but as soon as you are trained to use Report Box you can receive

reports from the public. INHOPE will send you a template as an example and you can view other hotlines' reporting pages by viewing the country reporting options on the INHOPE website.

6. **When do we start awareness-raising?**
   INHOPE can support and advise on this, and you can receive advice from INHOPE's communications department. There is no fixed timeline but once you are a provisional member you are invited to focus groups, webinars, bi-annual training meetings where all aspects of the needs of INHOPE hotlines are addressed with relevant trainings for hotline staff, analysts, managers, comms staff and more.

7.2 Technical FAQ

Technical FAQs when establishing a hotline. Once a hotline becomes an INHOPE member, they get access to ICCAM. This is a list of frequently asked questions received from staff responsible for the technical aspects of setting-up a hotline. We hope that they can help answer some of your questions when setting-up a hotline.

1. **What does a report consist of?**
   The report must contain at least one URL, this is the minimum information in order to create a new report. Hotlines receive reports through a reporting form on their website. This URL is assessed by a hotline analyst and if the analyst suspects there is CSAM on the URL, it is inserted into ICCAM.
   From this URL, the ICCAM platform determines the country of hosting and the number of media items hosted on the URL. The system downloads the **images and videos** found on that URL. These are called **content items in ICCAM**.

2. **What is report assessment?**
   Once the images and videos are downloaded in the system, the analyst can see them on their screen. The analyst then needs to provide an assessment of what they see. This means that they indicate the illegality of the content items. They will assess whether the content items are illegal everywhere (INTERPOL classification), or illegal according to national legislation. The values of assessment can be: Baseline, National, Doubtful, Not Illegal. Analysts learn how to use ICCAM during INHOPE's CORE training. Analysts learn how to assess the illegality of content items during INTERPOL's content assessment training, also provided by INHOPE.

3. **What is ICCAM and how does it benefit hotlines?**
   ICCAM is a technical platform that enables a secure exchange of reports of suspected CSAM between nationally established hotlines. ICCAM is an acronym that stands for "I C (see) Child Abuse Material". It was developed with funding from the European Commission.

ICCAM benefits its member hotlines in a few ways: It allows for a secure exchange of illegal material, and it reduces the exposure to already assessed content. If a content item has already been classified in the past, another hotline analyst does not have to classify it again. This minimises the exposure of hotline analysts to harmful content.

4. **How does an analyst use ICCAM?**

   ICCAM can be used in two ways: 1) via the user interface (UI) through a website (with a security certificate), and 2) via the API as a system-to-system connection.

   API stands for Application Programming Interface. An API is a software intermediary that allows two applications to talk to each other. In other words, an API is the messenger that delivers your request to the provider that you're requesting it from and then delivers the response back to you.

   The cases described in this technical FAQ refer primarily to the UI use of ICCAM (1).

   In order to connect to ICCAM, a new hotline should request access through iccam@inhope.org.

5. **How are reports exchanged in ICCAM?**

   When a report is entered into ICCAM, the system crawls (downloads) all content items found on that URL. Each URL is hosted at an Electronic Service Provider in a specific country. ICCAM calculates this automatically and provides the analyst with hosting information. All content items are assessed by the analyst and once assessed as illegal, the URL with the content item is sent to the hotline in the hosting country, directly via ICCAM. A national hotline only sees content items hosted within their own jurisdiction. Consequently, they can make a final assessment and if necessary, issue a notice and takedown order.

6. **How does notice and takedown work?**

   National hotlines have the mandate to issue notice and takedown orders within their national jurisdiction. This means that they inform the hosting company of the discovered CSAM and demand that the content is taken down. This process usually happens with a mutual agreement with the law enforcement authority in the country. For a detailed explanation of Notice and Takedown procedures, please check INHOPE's publication.

7. **Who should the hotline send a report to, when it receives a report hosted outside their national jurisdiction?**

   After a hotline analyst receives a report from the public, they trace the hosting location. If the analyst confirms that the hosting location is in another country, they insert the URL into ICCAM.

   ICCAM automatically checks the hosting country and sends it in real-time to the hotline analyst in that country.

   The information sent to the analyst in the hosting country is all data available in ICCAM of that report: e.g., URLs, images and videos, any classification made, name of analyst & hotline submitting the report.

   The analyst in the national hotline where the URL is hosted, confirms the illegality of the material in ICCAM. Afterwards they follow their Notice and Takedown Procedures according to national jurisdiction.

This means that the URL can be sent to the national Law Enforcement Agency, and a Notice and Takedown Order is sent to the Hosting Provider either by the hotline or by the Law Enforcement Agency. The information sent can be, but it is not limited to: Time and date of receiving the report, the URL, any other useful information corresponding to the report (either provided by the reporter or by the hotline), classification of the report: what is the illegality and any other attributes.

8. **What information, other than URLs, will be transmitted from INHOPE/member hotlines to the national hotline via ICCAM?**

   The report information contains: IP address, hosting country, name of hosting company, time and date of submission, cookie and referrer required to reproduce the site (optional), memo (optional, used to guide the analyst processing the report), username and password (optional), commerciality of the website (optional), type of website, Each content item also is sent with a classification on age of the victim depicted in the content item (mandatory), gender of the victim (mandatory), illegality classification (mandatory). Additionally, information is shared whether the URL and content item have already been sent to a law enforcement agency in the receiving country or if a Notice and Takedown Order has already been sent before.

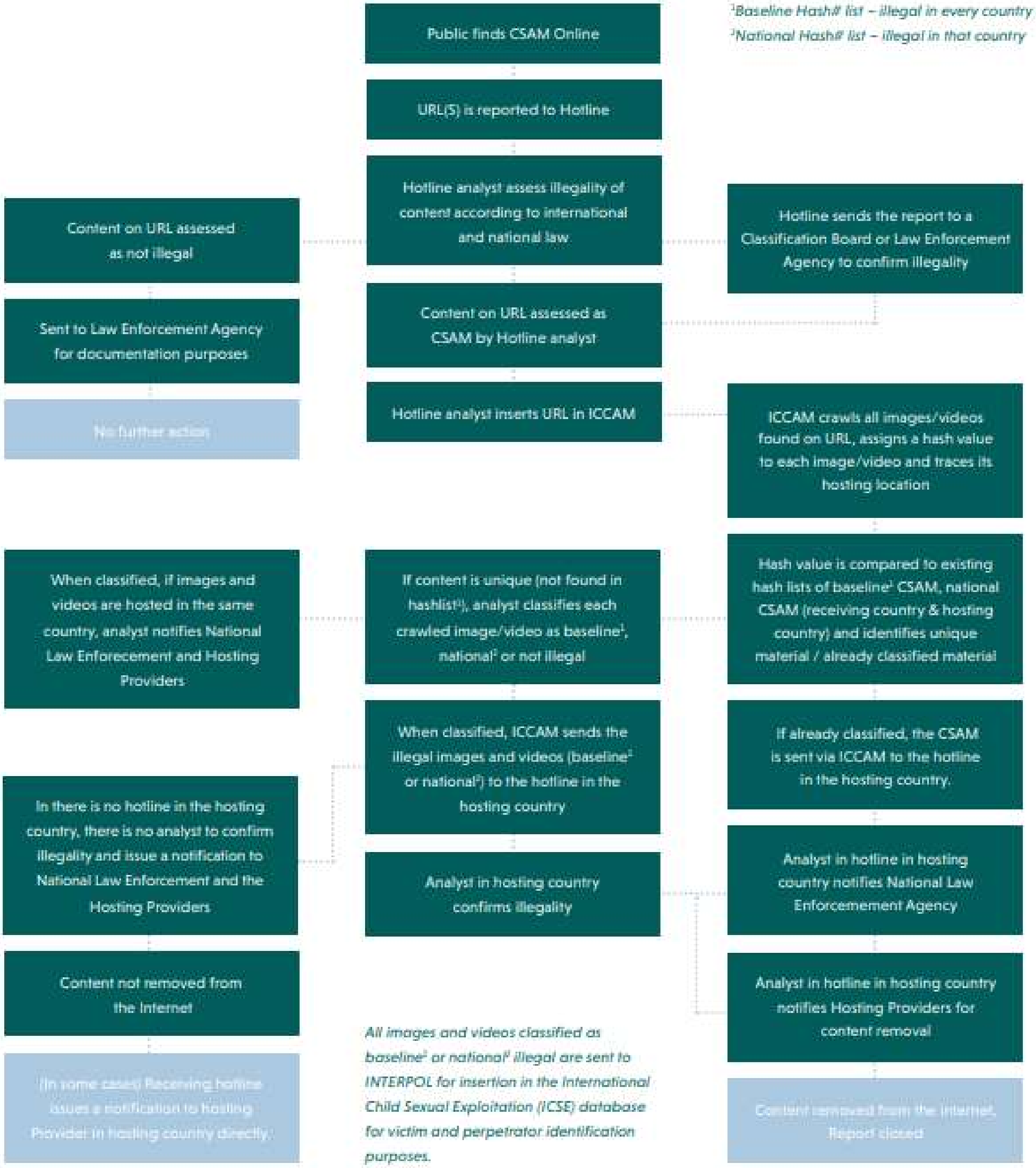
9. **Who is responsible for submitting URLs to INTERPOL's International Worst of List (IWOL)?**

   INHOPE is responsible for sharing CSAM reports with INTERPOL. Subsequently, INTERPOL reviews the reports, and where applicable, adds them to the International Worst of List (IWOL). Every image and video inserted into ICCAM and classified as illegal is shared with INTERPOL. This means that INTERPOL reviews this material and where applicable, adds it to their International Child Sexual Exploitation Database (ICSE) for further international victim identification.

10. **Is ICCAM hosted by the hotline?**

    No, ICCAM is hosted by INHOPE. The system is developed and maintained by a Dutch technical company, ZiuZ (https://www.ziuz.com/). The servers of ICCAM, who contain all material exchanged between the hotlines, are stored at INTERPOL's headquarters in Lyon, France.

    See on the next page a detailed overview of the process that takes place within ICCAM.



[1]Baseline Hash# list – illegal in every country
[2]National Hash# list – illegal in that country

Public finds CSAM Online

URL(S) is reported to Hotline

Hotline analyst assess illegality of content according to international and national law

Content on URL assessed as not illegal

Sent to Law Enforcement Agency for documentation purposes

No further action

Hotline sends the report to a Classification Board or Law Enforcement Agency to confirm illegality

Content on URL assessed as CSAM by Hotline analyst

Hotline analyst inserts URL in ICCAM

ICCAM crawls all images/videos found on URL, assigns a hash value to each image/video and traces its hosting location

Hash value is compared to existing hash lists of baseline[1] CSAM, national CSAM (receiving country & hosting country) and identifies unique material / already classified material

If content is unique (not found in hashlist[1,2]), analyst classifies each crawled image/video as baseline[1], national[2] or not illegal

When classified, if images and videos are hosted in the same country, analyst notifies National Law Enforecement and Hosting Providers

If already classified, the CSAM is sent via ICCAM to the hotline in the hosting country.

When classified, ICCAM sends the illegal images and videos (baseline[1] or national[2]) to the hotline in the hosting country

In there is no hotline in the hosting country, there is no analyst to confirm illegality and issue a notification to National Law Enforcement and the Hosting Providers

Content not removed from the Internet

(In some cases) Receiving hotline issues a notification to hosting Provider in hosting country directly.

Analyst in hosting country confirms illegality

Analyst in hotline in hosting country notifies National Law Enforcemement Agency

Analyst in hotline in hosting country notifies Hosting Providers for content removal

Content removed from the internet. Report closed

All images and videos classified as baseline[1] or national[2] illegal are sent to INTERPOL for insertion in the International Child Sexual Exploitation (ICSE) database for victim and perpetrator identification purposes.

11. **What happens when a report received from the general public is a duplicate? How can an analyst check if the content is already in ICCAM?**

    When a URL is inserted into ICCAM, a page is crawled, and all individual media files are downloaded into the system. At that point, a hash value is created and saved of every single media file.

    Hashing is the process of using an algorithm to assign a unique hash value (long number) to an image. Duplicate copies of the image all have the exact same hash value. For this reason, it is sometimes referred to as a 'digital fingerprint'. Hash matching takes place automatically in the background in ICCAM. When an image or video has been inserted into the system before, the system matches the hash value and informs the analyst that this content item has been seen before and what the given classification is.

    There are two automated checks that take place in ICCAM i.e., 1) with the reported URL and 2) the hash value of the image and/or video. Firstly, ICCAM automatically checks if the reported URL with the same IP address has been inserted in the previous five days. If it has been inserted, the report is closed automatically as it is considered that the hosting hotline has already processed that URL. The second automated check takes place with the hash value of the images and videos found on the reported URL. The system automatically checks if the hash value of any image or video has been stored in the system before. If the answer is yes, the item is automatically classified, and the content analyst does not need to make an assessment on previously seen content. In cases where the content item is classified as baseline (internationally illegal according to INTERPOL’s criteria), the image/video appears blurred on the analysts’ page to limit exposure to harmful content to more analysts.

12. **Who is the owner of the data exchanged within ICCAM?**

    Each hotline who inserts URLs into ICCAM is owner of that data. Any URL that is inserted by another hotline, but hosted in your country, is your ownership too. Once a hotline becomes an INHOPE member, this is regulated by the ICCAM Participation Agreement. This document sets out the data sharing rules, in particular regarding contributing, accessing, changing, storing, deleting and/or sending information. This document must be signed by all hotlines before they start using ICCAM.

13. **What is the duration for which the national hotline is required to maintain data of reports received and generated, according to INHOPE guidelines/rules, after the offending material has been taken down by the government or intermediary (ISP, hosting provider, etc.)? Does this data include content that is classified as CSAM?**

    The ICCAM Data Retention rules can be seen in the table below. These rules are set according to Dutch Data Protection Regulations. Each hotline should seek legal advice for the national regulations on data retention in their own country.

Type of data	Retention Period/Remove/Keep?
Analysts	
Name	1 year after report closed
Email	1 year after report closed
Phone number	1 year after report closed
Hotline	
Name	Keep (name of hotline not personal data)
Manager Email	Change to general email address of hotline once Manager leaves e.g., info@.com
Manager Name	Change to hotline name once Manager leaves.
Website	Keep
Report	
Website/Content URL	10 years
Website/Content IP Address	10 years
Website/Content ISP	10 years
Memo	n/a
Referrer URL	10 years
Content	
Content URL	10 years
Content IP Address	10 years
Content ISP	10 years
Memo	n/a
SHA1 Hash	30 years
MD5 Hash	30 years
Gender	10 years
Age Group	10 years
Ethnicity	10 years
Other content details (Virtual/Modeling/UserGenerated)	10 years
Hash matching	
SHA1 Hash	30 years
MD5 Hash	30 years