

CSAM Policy

In the course of our investigative work there are times where we might locate content that is, by its very nature, illegal. If we are investigating crimes such as child exploitation this might be intentional, in which case we should be fully trained on how to appropriately handle that digital evidence. Investigative units that focus on that type of work are less an issue than those who unintentionally stumble onto digital contraband and find themselves unprepared to deal with the ramifications. Those who work specifically in roles investigating child exploitation will already have more detailed process and policies in place.

Although there is a range of digital contraband that could potentially fall into this category, the most critical issue to address in your process and policy is child sexual abuse material (CSAM). Within the open-source intelligence community specifically, the increase in crowd sourced programs investigating missing or exploited persons has increased the chances that less experienced investigators may find themselves in a situation where they locate material with a reporting requirement. I am not an attorney, but for US based investigators I would recommend familiarizing yourself with **Title 18 Part 1 Chapter 110 Section of 2258A** of the US legal code. (<https://www.law.cornell.edu/uscode/text/18/2258A>)

There are a couple of important distinctions when it comes to CSAM regarding semantics. Many laws in the US and elsewhere still use the term “child pornography” which is widely considered to be outdated and inaccurate. Although you may need to use that terminology in the charging documents required by your jurisdiction, I recommend using the term “child sexual abuse material” in your notes and incident documentation. This or the acronym CSAM are generally accepted as the preferred terminology.

So first let us address what you should do if you stumble onto some content that you feel may be CSAM or otherwise bear an inherent reporting responsibility. The following are some recommendations for those who do not already have a process or policy in place.

1) Do not capture it – Although typically when we find potential evidence of a crime, we immediately capture it for preservation, there are two primary reasons to avoid capturing CSAM. The first is to protect the victims. The last thing we want is unnecessary copies of harmful material being created and possibly leaked due to mishandling or a security compromise. The second is that in many jurisdictions, mere possession of CSAM images and video are a felony. Although your intentions may be noble, collecting this material if it is not your authorized duty could create legal consequences. If you are trained to handle evidence in these types of investigations, follow your defined procedure, otherwise it is best to record URLs and other non-graphic material only.

2) Notify a supervisor – Due diligence is essential in these incidents and one of your first actions should be notifying a superior so that they can ensure that all appropriate procedure and policy requirements are followed. They may have additional responsibilities related to the scenario that you are unaware of. Even if mistakes are made along the way, we must show that we made every effort to act in good faith.

3) Report the incident to law enforcement – Reporting requirements will vary between jurisdictions, but ethical responsibilities for reporting are universal. Although your local law enforcement agency may not have the capabilities to investigate the incident fully, you will have created a record and paper trail which demonstrate due diligence personally and on behalf of your organization.

4) Report the incident to NCMEC – Report the content to the National Center for Missing & Exploited Children (<https://www.missingkids.org/gethelpnow/cybertipline>) Memorialize this reporting in your notes and consider saving a screen shot of your submission.

5) Report it to the involved platform – The timing and appropriateness of this will depend on the platform. If the platform itself is potentially involved in the criminal activity, we do not want to tip our hand. Also, we

want to make sure that we notify law enforcement first so that they have an opportunity to preserve evidence. Most platforms will retain digital evidence in CSAM incidents, but not all. Law enforcement will often serve the platform legal unit with a preservation letter to request that an offline backup is maintained while executing content removal.

6) Document the incident – Create a concise record to memorialize encountering the contraband material. If you are uncertain what to include, consider the following: Date/Time, Investigator, Screening Supervisor, URLs where evidence may be located, concise description of the contents in common language (you are conveying an understanding of why you believe the material may be contraband).

7) Wellness – Even for seasoned investigators, exposure to CSAM or other materials depicting victimization can be very disturbing and there can be lasting personal emotional impacts if not properly addressed. It is entirely appropriate to speak with a professional counselor or other support personnel following an exposure to images, video, and even secondhand accounts of inhumane acts. It is important to take care of yourself, subordinates, and colleagues following a CSAM exposure whether due to an investigation or an unintentional discovery while doing other online research.

The largest pitfalls in properly handling this material is in the reporting. Again, we do not create copies of the photos or videos unless we are trained to do so. We want to document enough information to direct authorities to intervene and yet we want to be certain that we are not making things worse for the victim(s).

These recommendations are not a replacement for preparing a proper and well-defined procedure for handling illegal digital material. Although I am not a believer in having policy just for the sake of policy, this is an area of potential liability and you would be wise to consider a written policy reflecting and supporting your prescribed best practices. You could end up needing to defend yourself or a colleague against allegations of criminal or negligent behavior, and if that occurs a written policy shows your organization is professional and squared away. Below is a very general framework for a CSAM policy.

Sample CSAM Policy

SECTION 1.1 – REPORTING EXPLICIT MATERIAL

Employees in the course of their normal duties may encounter materials on the internet which by their very nature demand action regarding notifications and proper handling. This policy aims to provide a baseline set of procedures which support the proper handling of any incident involving illegal digital content and/or specifically child sexual abuse material (CSAM).

1.1 DEFINITIONS

[If not addressed elsewhere in the section]

CSAM – Child sexual abuse material consists of any still, video, or audio data depicting a any visual depiction of sexually explicit conduct involving a minor.

Media – Visual or audio material stored in an analogue or digital format.

Minor – An individual whose appearance would lead a reasonable person to believe they were under 18 years of age.

1.2 REPORTING RESPONSIBILITIES

Instances of illegal online content to include CSAM will be reported to the appropriate legal authority. Additionally, employees will notify a supervisor immediately upon discovering said content. The supervisor will document the incident and ensure that material which is exploitive in nature is not further propagated.

1.3 POST INCIDENT PROCEDURES

Equipment exposed to sensitive and potentially illegal material will be examined by appropriate technology personnel to ensure that any digital contraband is removed and that the workstation or systems in question are appropriately sanitized prior to further use.

1.4 DOCUMENTATION

Personnel will not copy or otherwise reproduce any material that is believed to be child sexual abuse material. Every effort will be made to capture location information such as internet addresses, IP addresses, and/or domain names without including any media that could cause further exposure or harm to the depicted victim.

1.5 EXCEPTIONS

This policy does not supersede any policy or procedures related specifically and directly to investigative units with child exploitation investigations as a primary duty. Such units must have specific exemption granted by a the [Unit or Section Commander].

1.6 TRAINING

All employees are responsible for reviewing and acknowledging this policy. Any units assigned with online investigations as a primary duty will complete an additional body of training at the discretion of their unit commander.

1.7 REVISION HISTORY

*Legacy versions of this policy which are typically presented in reverse chronological order.

Rev. 20.10 [Link to official archive if applicable] [Date of inception]-[Date Rescinded]

1.8 APPENDIX

[Appendices are used for informational material that is helpful, but not directly related to the implementation of the policy. These can be references to related policies/procedures or case law providing the foundation for investigative best practices.]

Once you have a policy drafted it is wise to have it reviewed by your in-house council or other legal advisory body. Do not forget to provide training for employees on both the policy and procedures. A baseline of awareness will save you a fair amount of stress when an incident involving CSAM occurs during an investigation or intelligence operation. If you are a student or non-professional OSINT practitioner, consider starting up a conversation with your instructors and peers about the proper handling of illicit materials. If you join a crowd sourced or charity event related to crimes against children, please ask the organizers for direction and education regarding appropriate procedures for responding to occurrences of CSAM or other digital contraband. As with most other aspects of online investigations, the key is having a plan and showing that a reasonable level of due diligence was carried out.