

Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG Disposition of Child Sexual Abuse Materials

Best Common Practices

February 27, 2015

Legal Disclaimer

This document is not legal advice. M³AAWG strongly suggests that readers work with their company's legal counsel or avail themselves of independent legal advice regarding their rights, responsibilities and obligations relevant to prevailing legal jurisdictions.

Individual employees should have specific CSAM (Child Sexual Abuse Materials) handling protocols provided to them in writing by their employers. Employers must provide such protocols and must ensure that waivers – typically allowing for a potentially hostile work environment due to exposure to these materials – are signed by those employees whose role involve any potential exposure. Additional requirements, such as mandatory law enforcement notification, may also be part of the protocol and the complete protocol must be developed with the advice of competent legal counsel.

I. Introduction

It is an unfortunate reality that Internet anti-abuse professionals are, from time to time, encountering child sexual abuse material in the course of their work.

It is *critical* that incidents be dealt with expeditiously in a legally compliant manner, especially to avoid inadvertent self-incrimination. All staff that may be impacted by such incidents must be given appropriate training and access to support resources **prior** to the possibility of these types of events occurring.

II. Terminology and Definition

CSAM - Child Sexual Abuse Material

CSAM is often discussed using a number of other terms, such as “child porn” or “kiddie porn,” which should be avoided as they minimize the impact of this material both on the children involved and within society in general. More accurate alternative definitions provided by [INTERPOL](#)¹ include:

- Documented child sexual abuse
- Child sexual exploitive material
- Depicted child sexual abuse
- Child abuse images

Spamhaus includes the abbreviations "[CAM](#)"(Child Abuse Material), "[CEM](#)"(Child Exploitative Material) and "[CAI](#)" (Child Abuse Images)².

While the definition of CSAM varies slightly from jurisdiction to jurisdiction, the following “Definition of Child Abuse Sexual Material in the United States” from The Technology Coalition’s [Employee Resilience Guidebook for Handling Child Sexual Abuse Images³](#), starting on page 3 and continuing on page 4 can be used as a baseline guide:

“... any visual depiction of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Sexually explicit conduct includes graphic sexual intercourse, such as bestiality, masturbation or sadistic or masochistic abuse. It also includes lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited or any graphic or simulated lascivious exhibition of the genitals or pubic area . . .

[continuing on page 4 under Reporting to the National Center for Missing & Exploited Children]

- possession, manufacture and distribution of CSAM;
- online enticement of children for sexual acts;
- child prostitution;
- sex tourism involving children;
- extra-familial child sexual molestation;
- unsolicited obscene material sent to a child;
- misleading domain names; and
- misleading words or digital images on the Internet.”

III. Protocol for Personnel Involved in the Disposition of Child Abuse Reports

Any anti-abuse professional who is unsure if any material is CSAM should report it to law enforcement. Do not take a chance. It is not up to you to make this determination and it is best to err on the side of caution. Report the material to law enforcement immediately. It is important to note that CSAM reports **must** be filed with law enforcement as quickly as possible given that the abuse may be ongoing and the real-world impact of any delay can be horrendously dangerous.

Do not share materials, including images, video and URLs, with anyone except law enforcement – not your colleagues, not your boss. An incident report should be filed, but direct pointers or examples **must** be redacted. Be aware that distribution, even in incident reports, is illegal in many jurisdictions. The [Employee Resilience Guidebook³](#) states on page 4:

“Providers of electronic communication services and remote computing services must make a report ... when the provider has actual knowledge of any facts and circumstances of a violation of child sexual exploitation laws that involves apparent child pornography – e.g., the production, distribution, or possession of apparent child pornography; misleading domain names; and the obscene visual depiction of a minor.”

IV. Protect Yourself

Viewing CSAM materials is often a traumatic experience for those who do so in a professional capacity. There is no such thing as a wrong emotional reaction, nor is there anything wrong with seeking support and

assistance in dealing with the emotions that can arise. Your employer may have an employee assistance program, an insured psychology or psychiatry service, or you may prefer your own private services at a local hospital or clinic. Having a trusted professional to whom you can express natural reactions to such a situation is entirely appropriate and you are encouraged to have a support system in place preemptively.

Not everybody is “built” for this kind of work; in fact, few can do so for any period of time. It is not a personal failing if you decide you do not want to possibly be exposed to such incidents, nor if you wish to stop after having been exposed.

V. Reporting

It is strongly suggested that reports be made directly to the organizations listed by country at INHOPE.org⁴, some of which are reporting centers who will in turn report to law enforcement. If your country is not listed there, reports should be made to your national police or law enforcement agencies.

VI. Resources for Anti-Abuse Staff and Employers

1. **The Technology Coalition Employee Resilience Guide**
<http://technologycoalition.org/wp-content/uploads/2013/05/EmployeeResilienceGuidebook2013.pdf>
2. **M³AAWG Abuse Desk Common Practices**
https://maawg.org/sites/maawg/files/news/MAAWG_Abuse_Desk_Common_Practices.pdf
3. **Suicide Crisis Hotlines**
http://en.wikipedia.org/wiki/List_of_suicide_crisis_lines
4. **Initiatives**
 - (a) **Microsoft PhotoDNA**
<http://news.microsoft.com/presskits/photodna/>
 - (b) **Google Search Engine Shared Database**
<http://telegraph.co.uk/technology/google/10122452/Google-builds-new-system-to-eradicate-child-porn-images-from-the-web.html>

VII. Conclusion

The intersection of CSAM with anti-abuse personnel is infrequent, but when it occurs, it is of the highest priority and requires very specific disposition. M³AAWG encourages readers of this document to delve further into the resources mentioned herein to gain a complete understanding of this issue.

VIII. References and Endnotes

¹See INTERPOL website Crimes against children, Appropriate terminology, <http://www.interpol.int/Crime-areas/Crimes-against-children/Appropriate-terminology>

²See the Spamhaus website, Frequently Asked Questions, “Criminal Child Pornography (Abuse and Exploitation),” http://www.spamhaus.org/faq/section/Online_Scams

³The Technology Coalition’s *Employee Resilience Guidebook for Handling Child Sexual Abuse Images*, <http://technologycoalition.org/wp-content/uploads/2013/05/EmployeeResilienceGuidebook2013.pdf>

⁴International Association of Internet Hotlines (INHOPE), <http://inhope.org>

