



THE TECHNOLOGY
COALITION

EMPLOYEE RESILIENCE GUIDEBOOK

FOR HANDLING

CHILD SEXUAL ABUSE IMAGES

March 2013

www.technologycoalition.org

TABLE OF CONTENTS

• Introduction	2
• Disclaimer	3
• Legal Reporting and Obligations	3
• Safe Handling and Reporting Practices	6
• Why Focus on Employee Resilience?	7
• The Hiring Process	8
• Building an Employee Resilience Program	11
• Promoting “Self Care”	13
• Conclusion	14

INTRODUCTION

The Technology Coalition (www.technologycoalition.org) is powered by leaders in the Internet services sector. Formed in 2006, the Coalition’s vision is to eradicate online child sexual exploitation. The group’s strategy is to develop and deploy technology solutions that disrupt a person’s ability to use the Internet to exploit children or traffic in child pornography. The Technology Coalition works with the National Center for Missing & Exploited Children (NCMEC) and its sister agency, the International Centre for Missing & Exploited Children (ICMEC), to identify and propagate technology solutions that create effective disruption. Current members of the Technology Coalition are:

AOL Inc.
EarthLink, Inc.
Facebook
Google, Inc.
Microsoft Corporation
PayPal
Time Warner Cable
United Online, Inc.
Yahoo! Inc.

Complying with laws against online child sexual exploitation is an important and potentially challenging responsibility for companies that offer Internet services. This resource’s objective is to provide a high-level summary of an organization’s obligations

related to reporting apparent child pornography that may be on its systems. In addition, this resource offers a set of practices and guidelines to support those employees who have exposure to online child pornography in the course of their work. Organizations use a variety of names for programs to support employees in these functions including “Employee Wellness” and “Employee Safeguard” programs. The Technology Coalition has chosen to name this approach “Employee Resilience.”

Disclaimer

This guidebook is intended to provide insight and high-level industry practices and is not intended to provide legal advice. The reader should consult with his or her legal team on what the company’s obligations are in this area and whether or how it should implement these guidelines.

The specific practices and guidelines included in this document, which are offered in support of those employees who have exposure to online child pornography in the course of their work, are offered as samples for reference only and are not intended to represent the best or only approach to any particular issue. Neither the Technology Coalition nor any individuals or companies providing the practices or guidelines make any warranty or guarantee with regard to the accuracy, completeness or suitability of the practices and guidelines, and they assume no responsibility or liability in connection with their use or misuse in a particular circumstance.

The Technology Coalition makes no warranties, expressed, implied, or statutory, as to the information in this guidebook.

Complying with all applicable copyright laws is the reader’s responsibility. This report may be freely redistributed in its entirety at no charge provided that any legal notices, including all copyright notices, are not removed. It may not be sold for profit or used in commercial documents without the written permission of the Technology Coalition, which may be withheld in the Technology Coalition’s sole discretion.

LEGAL REPORTING AND OBLIGATIONS

Definition of Child Pornography in the United States

Under federal law, Title 18 U.S.C. §2256, “child pornography” means 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.

Additional references on child pornography law can be found on the website of the Legal Information Institute at Cornell University <http://www.law.cornell.edu>. The National Center for Missing and Exploited Children (NCMEC) also has a summary of laws related to child pornography at <http://www.missingkids.com/home>.

Federal law, Title 18 U.S.C. §2258A, covers reporting requirements of electronic communication service providers and remote computing service providers.

Reporting to the National Center for Missing & Exploited Children

The National Center for Missing & Exploited Children (NCMEC) is a private, nonprofit organization that serves as the resource for the United States on the issues of missing and sexually exploited children. As a public-private partnership it is funded in part by Congress and in part by the private sector.

Under its Congressional mandate, NCMEC operates the CyberTipline, the national clearinghouse for leads and tips regarding crimes against children on the Internet. It receives reports in eight categories of crimes against children:

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

These reports are made by electronic communication service providers and remote computing service providers, who are required by law to report apparent child pornography to the CyberTipline (18 U.S.C. §2258A). Members of the public also make reports into the CyberTipline. The CyberTipline (www.cybertipline.com; 1-800-843-5678) operates 24 hours a day and 7 days a week.

Providers of electronic communication services and remote computing services must make a report to NCMEC's CyberTipline 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). See 18 U.S.C. § 2251, 2251A, 2252, 2252A, 2252B, or 2260; 18 U.S.C. § 1466A.

A company can report suspected child exploitation incidents to www.cybertipline.com or 1-800-843-5678 along with the company's mailing address, telephone number, facsimile number, and the electronic mail address of an individual point of contact at the company. NCMEC also has a bulk reporting mechanism, for companies that handle a high volume of reports.

Information about the suspected incident that should be reported to NCMEC includes:

- Identifying information: Information about the involved user or customer, such as email address, IP address, or any other identifying information including self-reported identifying information.
- Historical reference of the incident: This may include any information related to when and how the user or customer uploaded, transmitted, or received apparent child pornography as well as when and how the material was reported or discovered, including the date, time stamp, and time zone.
- Geographic location of the user or website: IP address or verified billing address, or, if not available, area code, or zip code.
- Any images of apparent child pornography related to incident.
- Complete communication containing any image: This may include information on the transmission of the image or any other images, data or files attached to or contained in the reported communication.

Statistics

As of December 2012, the CyberTipline has received more than 1.7 million reports of suspected child sexual exploitation since it was launched in 1998. Of the eight types of child exploitation incidents that CyberTipline reports to receive, child pornography constitutes the vast majority.

Data Retention and Handling

Federal law, Title 18 U.S.C. §2258A, also requires that a company preserve the contents of its report for 90 days after NCMEC's receipt of the report. The company should preserve the contents of the report along with images, data, or other digital files that are commingled or interspersed among the reported images. Those materials must be kept in a secure location, which includes limiting access by employees to that material to the extent necessary to comply with the law.

Companies may also want to visit the website of the US Internet Service Provider Association (USISPA) to review its "Industry Sound Practices for Reporting Apparent Child Pornography." (<http://www.usispa.org/wp-content/uploads/2011/04/US-ISPA-Sound-Practices-Protect-Act.pdf>)

SAFE HANDLING AND REPORTING PRACTICES

This section covers guidelines for developing safe handling and reporting practices. These guidelines are generalized and may not cover all of a company's reporting obligations. Coordination should take place among a company's legal, engineering and other relevant teams to create a process that fulfills the organization's reporting obligations as well as keeps data secure. Here are several safe handling and reporting guidelines based on industry practice:

1) Build tools to facilitate the reporting process and ensure security in each step of compliance.

Limiting the amount of time employees are exposed to child pornography is key. NCMEC offers a batch reporting system so that reports can be sent by XML rather than by filling out individual forms on the NCMEC system. Using this option, as well as developing other abuse-review tools, can significantly decrease the amount of time that an employee must spend reviewing child pornography.

Keep the servers that the child pornography is preserved on secure. Limit the access to these servers to only the people involved in child pornography investigations. Consider providing a work space to the team that handles the child pornography investigation in an area that has little to no other traffic. Provide employees with privacy screens for their monitors.

2) Create clear and well-documented policies and processes.

Sample policies that a company might consider include:

- Identify specific individuals responsible for dealing with child pornography issues and require that they complete specific training.
- Require all employees handling child pornography to only do so from a corporate network.
- Establish a Child Safety Team that ensures that all new products and services comply with your company's child safety policies and legal obligations. This team could be a standalone team, or it could be a cross-functional team of representatives from relevant corporate functions.

3) Establish a well-informed team.

Before assigning child pornography investigations to an employee, be sure to get the employee's informed consent. This includes providing an appropriate level of information so the employee understands what the role entails without negatively impacting those who wouldn't want the job.

Whenever possible, it is important that all participation is voluntary. It is also important that employees are pre-briefed before starting the job. Pre-briefing employees should include an in-depth description of the type of content they will be seeing and what warning signs they should be looking for in terms of their own possible negative reaction to the material. They should be informed of what company support resources are available to them. It is also recommended that these employees be interviewed weekly, monthly or quarterly so they can discuss their experiences in the job.

Where the volume of material and company size warrant, a company should have a minimum of two people on the team investigating online child sexual exploitation. The company and the employees involved need to have backup for the function.

Many companies choose to centralize the team for child pornography investigation and reporting to limit the exposure to employees. This approach provides a more controlled environment.

Another option is to decentralize the function by expanding the responsibility of child pornography investigation across multiple teams and departments. While this increases exposure, the benefits include a more collaborative effort across multiple levels within the company so that there is emphasis on the importance of the role. In addition, it can promote a feeling of a company-wide commitment to combating the problem and more people can be involved cross-functionally in developing solutions.

4. Consider vendor policies.

If a company contracts with a third-party vendor to perform duties that will bring vendor employees in contact with child pornography, it is recommended that the contract with the vendor clearly outline requirements to: 1) keep the content secure; 2) limit unnecessary exposure; and 3) abide by all applicable laws, including those governing child pornography.

WHY FOCUS ON EMPLOYEE RESILIENCE?

A study conducted by the National Crime Squad in the United Kingdom reported that 76% of law enforcement officers surveyed reported feeling emotional distress in response to exposure to child abuse on the Internet. This same study, which was cosponsored by the UK's Association of Chief Police Officers (ACPO) demonstrated the need for employee support programs to help them manage the traumatic effects.

Recommendations from this study included:

- Having documented policies and procedures for staff viewing images of online child sexual exploitation and for identifying how this role and the individual should be managed.

- Maintaining open dialogue between managers and employees on the potential impacts and options for obtaining support.
- Creating transparent and robust hiring practices that adequately inform the potential employee of what type and how much potentially impactful content he/she will be exposed to.
- Providing counseling services that are readily and easily available to all staff members who are exposed to child pornography.

In 2007, NCMEC psychologist Juliet Francis published “Helping the Helpers: Minimizing the Psychological Impact of Investigators Viewing Objectionable Material.” In her study, she found that viewing child pornography in the course of investigating it could, “increase one’s risk of exposure to the effects of secondary trauma,” despite the professional and personal satisfaction the viewer may garner from having such a noble task of fighting against it. (Source: <http://www.scribd.com/doc/24133366/Judith-AReisman-PhD-Picture-Poison>).

As noted in NCMEC’s “Helping the Helpers” study, helpers “have formed an empathetic engagement with a victim’s trauma and as a result become vicariously traumatized.” This can result in “feelings of incompetence and hopelessness regarding one’s abilities to help others, challenges to one’s faith, a heightened sense of personal vulnerability, as well as distrust and cynicism about the human condition.”

The same document points out that secondary trauma is associated with higher employee turnover as well as increased employee sick leave and physical illness.

Employee morale and longevity are important issues for any organization and it is no different for the department that handles the reporting of apparent child pornography. The company and the function benefit by having staff members with the experience and knowledge to handle these functions efficiently.

THE HIRING PROCESS

Industries, such as law enforcement and emergency services, that require employees to be exposed to traumatic events or images have long understood the cause and effects of secondary trauma. Many have robust programs and policies to mitigate the impact on employees. The Internet industry is recognizing that a similar approach should be considered for employees who are viewing child pornography.

The broader concept of Employee Resilience starts with the hiring process.

Whenever possible these roles should be staffed voluntarily by employees who clearly understand what type of content they will be exposed to.

Regardless of whether an employee has volunteered for a position or, out of necessity, has been placed in a position where exposure to potentially impactful content will occur, it is important to be transparent throughout the hiring process about what type of content he/she could potentially be exposed to. Additionally it is important to set realistic expectations about how much exposure the employee can expect in his/her role. Some care needs to be taken to adequately prepare the employee without traumatizing or overwhelming him/her before he/she even starts in the position.

Some helpful resources to use when educating a candidate on what to expect include:

- The legal definition of child pornography, as codified in 18 U.S.C. §2256.
- The NCMEC website <http://www.missingkids.com/home>
- Internet Watch Foundation (IWF) <http://www.iwf.org.uk/>
- Child Exploitation and Online Protection Centre (CEOP) <http://ceop.police.uk/>

A company should consider adjusting the level of transparency throughout the hiring process, based on the candidate’s previous experience, comfort level and expected exposure level in the role. The following are two examples of possible hiring process transparency plans:

Candidate A		Candidate B	
Previous experience	Role/ Exposure	Previous experience	Role/ Exposure
Program manager in the tech industry who has volunteered at homeless shelter.	Programmatic support to operations team that handles content. Zero to minimal exposure to actual content, but daily exposure to discussions of content. Role will require knowledge of online child sexual exploitation.	Ex-social worker who specialized in abused children cases.	Operations team member who will be handling online child pornography on a daily basis.
Transparent Hiring Plan		Transparent Hiring Plan	
Informational interview	<ol style="list-style-type: none"> 1. Use industry terms like “child pornography” and “online child sexual exploitation” to describe subject matter. 2. Encourage candidate to go to websites (NCMEC, IWF, CEOP, etc.) to learn about the problem. 	Informational interview	<ol style="list-style-type: none"> 1. Use industry terms like “child pornography” and “online child sexual exploitation” to describe subject matter. 2. Encourage candidate to go to websites (NCMEC, IWF, CEOP, etc.) to learn about the problem.
Follow up interviews	<ol style="list-style-type: none"> 1. Discuss candidate’s previous experience/knowledge 	Follow up interviews	<ol style="list-style-type: none"> 1. Discuss candidate’s previous experience/knowledge

	<p>with this type of content.</p> <ol style="list-style-type: none"> 2. Discuss candidate's current level of comfort after learning more about the subject. 3. Allow candidate to talk with employees who handle content about their experience, coping methods, etc. (*Note: caution employees to not disclose explicit examples of content.) 4. Be sure to discuss any voluntary and/or mandatory counseling programs that will be provided if candidate is hired. 		<p>with this type of content.</p> <ol style="list-style-type: none"> 2. Discuss candidate's current level of comfort after learning more about the subject. 3. Allow candidate to talk with employees who handle content about their experience, coping methods, etc. (*Note: caution employees to not disclose explicit examples of content.) 4. Be sure to discuss any voluntary and/or mandatory counseling programs that will be provided if candidate is hired. 5. Point candidate to the PROTECT Our Children Act of 2008 if they are not already familiar with it. Caution the candidate that the legal definitions in the Act are very explicit and detailed.
After hiring	<ol style="list-style-type: none"> 1. Provide internal documentation on policies, content scenarios, etc., including an in-depth tutorial on the Protect our Children Act of 2008. <p>*Note: the legal definition of child pornography is explicit and detailed. New employees should be encouraged to make use of employee resilience services as needed.</p>	After hiring	<ol style="list-style-type: none"> 1. Provide internal documentation on policies, content scenarios, etc., including an in-depth tutorial on the Protect our Children Act of 2008. <p>*Note: the legal definition of child pornography is explicit and detailed. New employees should be encouraged to make use of employee resilience services as needed.</p> <ol style="list-style-type: none"> 2. In first week of employment, do a controlled content

			<p>exposure with the new employee along with seasoned team members and/or a counseling service provider.</p> <p>3. Set up post-exposure counseling sessions for employee.</p>
--	--	--	---

BUILDING AN EMPLOYEE RESILIENCE PROGRAM

If employees are going to be exposed to this type of content on a regular, ongoing basis as a function of their jobs, it is also important for the company to have a robust, formal “resilience” program in place to support an employee’s well-being and mitigate any effects of exposure.

Employee Resilience Programs should be tailored to fit the needs of the company and team. There is no “one size fits all” program and program developers should investigate a range of program designs. Factors to consider when designing an Employee Resilience Program include level of exposure, size of team, size of company, and available resources. Many companies have an Employee Assistance Program (EAP) that can be leveraged when developing individual safety plans and Employee Resilience Programs.

Group support sessions can also be helpful on a monthly or quarterly basis. These sessions help employees understand that they are not alone in their feelings and that support is available to them.

While some employees may initially discount or disregard resources to help them cope with the potential impacts of this work, it is important for their managers to communicate the benefits of taking time away from the work and examine whether or not they need to take advantage of available resources.

Designing a tailored Employee Resilience Program is important. There are, however, certain elements that are critical to the success of any Employee Resilience Program.

- The program should include elements (e.g., education, intervention, counseling services, and evaluation) that are administered by a professional with specialized training in trauma intervention, ideally secondary trauma if the specialty is available.
- The professional care provider should be an outside resource, not an employee of the company. This ensures confidentiality and helps remove barriers to open communication.
- Strong consideration should be given to making select elements of the program (such as counseling) mandatory for exposed employees. This removes any stigma

for employees who want to seek help and can increase employee awareness of the subtle, cumulative effects that regular exposure may produce.

Following are two examples of possible Employee Resilience Programs.

Company A: Small ESP that employs 300; handles a few child exploitive issues per month.	Company B: Large ISP and Social Networking services provider that employs 50,000; handles 50+ child exploitive issues per day.
Designate employees to handle issues.	Designate a centralized team to handle issues.
Develop shared workload plan, if warranted, such that no one person handles all apparent child pornography.	Develop shared workload plan, such that no one person handles all apparent child pornography.
Provide bi-annual education on the effects of exposure for employees (including supervisors), conducted by a professional specializing in secondary traumatic stress.	Provide mandatory monthly group counseling sessions for team.
Provide professional assistance in developing individual safety plans.	Provide mandatory quarterly individual counseling sessions for team members.
Provide access to emergency counseling services as needed by employees experiencing severe response.	Provide access to emergency counseling services as needed by employees experiencing severe response. Provide professional assistance in developing individual safety plans.
	Provide bi-annual education on the effects of exposure for employees (including supervisors), conducted by a professional specializing in secondary traumatic stress.

If your company contracts with vendors to perform online safety functions, consider using vendors that provide Employee Resilience programs for their employees who must handle child pornography as a regular part of their contracted duties.

PROMOTING “SELF CARE”

Another important principle that has been emphasized by professionals dealing with exposure to child pornography material is to focus on self-care, including both long-term stress reduction techniques and immediate coping plans in the case of traumatic exposure.

Long-term stress reduction refers to typical “wellness” activities and includes concepts like exercise, healthy diet, adequate sleep, and good work-life balance. These are well understood and widely-accepted concepts so this document won’t go into detail except to reiterate the importance of a healthy, balanced lifestyle to combat the potential emotional impacts of long-term exposure.

Employees at risk for exposure to potentially traumatic content should have a personal plan to help them cope with any immediate trauma responses. Having a personal safety plan to manage these responses may enable the employee to continue working on a critical project and could help mitigate the cumulative effects of repeated exposure.

It is important to note that a secondary traumatic stress response can occur after just one exposure to impactful content. Traumatic responses may include immediate or delayed expressions of grief or anger, a heightened sense of personal vulnerability, intrusive thoughts and difficulty sleeping.

Keep in mind that while this document addresses child pornography, employees can also be impacted by other types of content, such as violence against people or animals.

Safety plans are tailored to the individual. While there are various support resources available to help an employee develop his or her safety plan (e.g., managers, human resources, fellow employees), it is strongly recommended that safety plans be developed with assistance from a professional counselor who is trained in secondary traumatic stress.

Below is a sample safety plan. It includes a variety of activities that an employee may use depending on the depth of his or her reaction.

- Go for a 15-minute walk outside.
- Talk to a friend. (Designate specific person(s) and get consent from them ahead of time.)
- Do a different work activity for an hour.
- Go home. (Requires pre-planning and open dialogue with manager.)
- Participate in a team or group activity outside of work.
- Engage in a hobby or in a physical activity requiring concentration.
- Call counselor. (This could be an Employee Assistance Program, public hotline, or personal care provider.)
- Take time off. (Discuss with manager.)

Having a tailored, detailed personal safety plan can greatly enhance an employee's ability to manage any secondary traumatic stress that may occur from exposure to online child pornography.

CONCLUSION

Responsible members of the Internet industry are actively meeting their obligations to report apparent child pornography on their systems in order for NCMEC, law enforcement and others to pursue the appropriate action to help keep children safe. In addition to developing technology tools, the industry recognizes that it must support those employees who are on the front lines of this battle. It is the hope of the Technology Coalition that this guidebook and suggested resources enhance those efforts.

www.technologycoalition.org