Tech Coalition

Responding to disclosures of child sexual exploitation and abuse through AI systems

Practical guidance for AI responses and company action

Commissioned by

ANTHROP\C Google OpenAI

Executive summary

Child sexual exploitation and abuse (CSEA) is widespread and often never disclosed. UNICEF estimates that around 1 in 8 girls and women and 1 in 11 boys and men worldwide experienced rape or sexual assault before age 18. Across countries with available data, around 7 in 10 young women aged 18–24 who experienced contact sexual violence in childhood had never told anyone [1]. Research with children in 21 countries found that more than 40% of cases of technology-facilitated sexual exploitation and abuse had gone undisclosed and fewer than 1% had been reported to police, a social worker or a helpline. The most common reason children gave for staying silent was not knowing where to go or who to tell [2].

AI systems may become the first or only place someone tells: in a 2026 Australian national study, more young people who had experienced online sexual victimization told an AI system than told police, teachers, or reporting lines [3].
A response to a survivor disclosure, from either human or AI systems, can help them continue their disclosures and reach safe human support, or deepen negative thoughts and discourage further help-seeking.

Drawing on research, consultation with 23 experts, and scenarios identified by Tech Coalition members, this resource gives companies practical guidance for responding to disclosures from children, adult survivors, and people concerned about others.

Six core principles apply to every response:

1. **Take harm seriously, without blame or doubt**
2. **Let the person lead**
3. **Ask only what safety and support require**
4. **Be calm, clear and honest**
5. **Help the person reach safe human support**
6. **Avoid further harm, including from data**

The guide applies these principles through a taxonomy for describing possible disclosures, guidance on recognizing them, good practice responses by who is disclosing and the level of risk, and guidance on human review, reporting, communication and evaluation.

1. About this guide

Purpose and scope

This guide offers good practices for technology companies responding to possible disclosures of CSEA through AI systems. It is intended to inform teams responsible for product design, AI behavior, policy, trust and safety, safeguarding and related company decisions.

This guidance is designed primarily for AI systems that interact with users through conversation, but the principles also apply where a disclosure arises through other products, such as image generation tools or search systems. How this guidance applies in practice will vary depending on the model or product, its role within the AI stack, its technical capabilities and constraints, and the context in which it is used. While there may be reference to legal obligations as they overlap with principles drawn from the evidence and expert input, no recommendations in this guide constitute legal advice.

This guide was created in response to questions raised by Tech Coalition member companies. Anthropic, Google, and OpenAI jointly commissioned and funded the work to produce this report. The Tech Coalition thanks them for their support, as well as the other member companies who contributed insights and scenarios.

The guidance provided relates to AI systems responding to CSEA disclosure: an interaction in which sexual abuse or exploitation of a child is described or indicated. This scope includes, but is not limited to:

- A person describing CSEA they have experienced, including an adult describing abuse during childhood.
- An account of someone else's experience of CSEA, or an account where it is unclear whose experience is described.

The following user interactions are outside the scope of this guide:

- General distress with no indication of child sexual abuse or exploitation.
- Young people's questions or requests concerning consensual or age appropriate sexual activity with peers where no indicators of abuse or exploitation are present.
- Disclosures from people describing their own harmful sexual thoughts or behavior.
- Adult experiences of sexual violence that occurred in adulthood.
- Non-sexual exploitation or coercion, where there is nothing indicating CSEA.
  - **Note:** Additional factors like self-harm, suicidal ideation, threats or extortion may co-occur with CSEA. These co-occurring harms may be relevant to understanding a CSEA victim's circumstances and risks.

How to use the guide

The guide is built in layers, moving from what good practices are to apply to every disclosure to what applies to specific situations and decisions. Companies can read it in order or go straight to the sections most relevant to their work.

Section 2 summarizes the evidence and expert input behind the guide.

Section 3 sets out the core principles that apply to every response, while **section 4** sets out the taxonomy of disclosure types and provides the necessary tools to apply the principles to specific situations.

Sections 5 to 7 cover key decision points for a company: **recognizing a possible disclosure (5)**, **responding to the person and supporting safety and human help (6)**, and **communicating what happens (7)**. Section 6 includes a handful of example scenarios.

Finally, **Section 8** covers testing responses for effectiveness.

Companies can apply this guidance now, and what they learn from doing so, including the results of testing, will shape future work on this subject.

2. Evidence and expert input

How the evidence base was developed

This guide brings together a rapid review of research and existing guidance, along with extended consultation with 23 experts across 20 interviews.

The review covered statutory and clinical guidance, practice standards from specialist services and helplines, forensic interviewing standards, and research with children, young people, and adult survivors.

The experts were asked to consider questions that remained unresolved in the evidence base and how these might apply in the context of AI. Their perspectives were diverse:

Expert perspectives

Expert perspectives included child safeguarding, forensic interviewing, clinical and survivor support, child helplines, prevention, online safety, and law enforcement.

Sectors represented

Sectors represented included civil society, academia, law enforcement, and helplines.

Countries represented

Experts were consulted from 7 countries: US, UK, Ireland, Netherlands, Finland, Australia, and India.

Note that the Tech Coalition provides these expert perspectives for informational purposes only and given the nature of the information, we encourage a diligent and independent review of these resources.

We want to thank the experts who shared their valuable knowledge through interviews. You can find a list of the experts who agreed to be named at the end of this resource.



2. Evidence and expert input

Evidence review

Limitations

Evidence on how an AI system should respond to disclosures, and whether its responses help, is very limited. Expert input was of limited breadth, survivors and young people were not consulted directly, and reporting guidance draws mainly on US arrangements. While evidence and expertise were drawn from a variety of regions, more needs to be done to understand any necessary variations for regional implementation.

Disclosure is usually a process, not a single statement. People tell gradually and test the response [4–7], describe harm without naming abuse [8], or speak through questions, stories, or accounts about friends [9, 10]. Disclosure may take years or decades [11]. A child being exploited may call the person exploiting them a boyfriend or girlfriend [12]. Retraction is common and does not mean abuse or harm did not occur, false allegations are rare, and guidance supports responding to partial accounts [4, 13, 14]. Several experts judged, with none disagreeing, that a story or account about a friend is likely to reflect something real, while an indirect signal is not proof.

The first response can shape further disclosure and help-seeking [4, 15, 16]. Belief is the most consistently recommended response, and the response should not adjudicate whether the account is true [9, 13, 17]. Children value belief, protection and support, and a child who firmly believes they are to blame may need to hear why it is not their fault [18]. Unsupportive responses are linked to self-blame and not telling again [4, 6, 19–22]. Survivors value control over when and what they share [23, 24]. Responses should use the person's own words as far as possible, including their terms for the person causing harm. Language should not imply consent, minimize harm or blame the child, or impose an identity such as "victim" or label their reactions or symptoms with a clinical diagnosis [9, 18, 25–28]. The core supportive response applies to children and adults, although safeguarding action and reporting choices differ between age groups [13, 24].

Support does not require investigation. A person receiving a disclosure listens and supports rather than investigating [9, 17]. Most experts addressing questioning, with none disagreeing, said AI systems should not lead, press for detail or gather evidence. The largest group of experts favored asking only the minimum needed for safety and suitable support. Experts differed on whether an AI system should ask for identifying or location details where harm is imminent and several said a platform should use information it already holds before asking for more. In general, questions that are asked should be open, short and one at a time [17, 29]. Acute stress can reduce working memory, so responses should be plain and given one piece at a time, and should avoid introducing extreme emotional words such as "terrified" with a child [18, 31, 32].

Honesty about confidentiality comes before a disclosure. Guidance says never promise secrecy or anything outside the responder's control [10, 17]; AI systems should not imply that 'help' has been contacted and is on its way [27, 28]. Confidentiality limits should be explained before disclosure, in language suited to the person's age [17, 33]. The largest group of experts favored explaining what happens to a conversation at the start; several warned against introducing this as a warning mid-disclosure. Text-based helplines minimize keeping records that may have to be released [34], although this may sit in contrast to other legal obligations on platforms [35].

Human help must be realistic and safe. Disclosure of current or ongoing abuse calls for immediate attention to safety without extracting a detailed account [36, 37]. Urgent risks such as self-harm are dealt with alongside the disclosure, not after it [37, 38], and after a recent assault a response can say that medical care exists and time matters [37, 39]. Experts and reporting guidance from the US National Center for Missing & Exploited Children (NCMEC) point to similar signals that call for urgent attention or escalation [40]:

- active abuse, or signs that new abuse material is being produced
- a planned meeting with the person causing harm
- active sextortion or coercion
- the person causing harm having physical access to the child, being nearby or planning to travel with them
- a child being offered for sexual exploitation
- a risk of self-harm.

Several experts held that the final judgment on urgency belongs with a person, with automated tools routing cases that show these specific signals to trained reviewers. Reporting frameworks give imminent risk the highest priority but set no single cut-off: reference points include 24 hours [41] and about 48 hours (one expert), with near-future risk the next priority [35]. Most experts saw human support as a main aim, preferably offered as part of the conversation, but noted that hasty referrals can reinforce shame [36] and abrupt endings may cause harm [42]. Services are best explained before they are named [10], and wherever possible should be local and in the person's language [43, 44]. Several experts

2. Evidence and expert input

warned that a referral is not an outcome: services an AI system points people to, such as helplines, should be vetted for reliability and capacity. Some noted that a report can also cause further harm if the child is not prepared or supported, or where local contexts make involving police risky. A young person who hears a friend's disclosure can be helped to pass on support and bring in a safe adult, who then acts [10, 11]. Caregivers and devices cannot be assumed to be safe [17, 34, 45, 46]. Guidance cautions against encouraging the person experiencing harm to confront the person causing it [10, 47]. A response should build safety planning on what the person already does and, where help is refused, keep options open [17, 24, 36, 48–50]. Experts agreed the AI should not keep pressing a route the person has declined, and that a safe alternative the person names themselves can be enough.

People may face different barriers to disclosure, but all should receive a supportive, nonjudgmental response. Barriers to disclosure may differ according to a person's disability, gender, race, culture, faith, sexual orientation and gender identity [17, 18, 51]. The following examples describe barriers and biases that AI systems should recognize and avoid reinforcing. Responders may overlook abuse when they attribute behavioral signs in disabled children to their disability [18]. Certain races, particularly Black children, may face bias by being seen as older or more responsible for what happens to them [17, 18, 26]. Boys may find it harder to recognize and disclose abuse due to masculinity norms that associate victimization with weakness or sexual experience as something to be prized [18, 52, 53]. Girls may face stigma and blame if they disclose [2, 17]. Statutory routes can themselves be a barrier for some First Nations families [54, 55]. Online abuse may come with additional measures of self-blame [9], in particular shame about sharing images [56] and fear of losing platform access [57]. Disclosures also come from friends, parents, and other worried adults, who face their own barriers: a parent may struggle to believe it and need to hear it is not their fault [10, 58]. Children harmed by other children may face additional pressure not to disclose, particularly when the other child is a sibling [58]. Not all sexual behavior between children is harmful, but an age gap of two years or more, inability to consent and coercion are indicators of abuse [58–60].

Sextortion calls for specific steps. Frontline guidance recommends reducing shame and panic, not paying or sending more images, stopping contact, keeping messages without copying images, reporting and blocking, and seeking human support [61, 62]. A young person is not at fault, even if they sent the first image, and a risk of self-harm should be taken seriously [62, 63]. Image-removal options depend on age, location and whether the person still has the image, and none guarantees removal [64–66].

What happens beyond the reply also matters. Notice of a report to authorities can restore control, while reporting without the person's knowledge can feel like betrayal and is linked to retraction [6, 18, 67]. Reports, notifications and follow-up can reach the person causing harm through shared devices or linked accounts [27, 68]. Reporting duties vary by country and role [69, 70], and several experts warned that systems should be designed to mitigate the risk of false or malicious reports intended to send police to someone's home. Guidance supports giving an adult the information to decide about reporting childhood abuse, and distinguishes that choice from safeguarding considerations where a child may be at risk now [13, 24, 70]; several experts favored asking what the survivor wants and offering reporting as one option, without implying they must report. Nearly half the minors in one US survey had used a platform below its minimum age, and fear of losing access deterred help-seeking [57]. What is kept and for how long remains unsettled: text-based and survivor services minimize records because they may have to be released or compelled in court [34, 46, 68], while reporting duties require records [35].

AI adds distinct limitations and risks. Risk can accumulate across turns and sessions without appearing in a single message [42]. Reliance on an AI system for support is a recognized risk, and comfort from it can delay seeking help from a person [28, 42]. Experts acknowledged this risk but were undecided on whether tone and response length should change where a person returned repeatedly with the same disclosure. Several indicated that where possible, a model should not answer repeated returns with an identical stock response or turn abruptly cold, and should acknowledge what was said before where the product remembers it. Role-playing was another risk identified by experts: none supported the AI roleplaying abuse for any reason, most of those asked preferred the response to provide guidance on how to tell a safe person over roleplaying help-seeking.

3. Core principles

These six principles can apply to every response to a possible CSEA disclosure, whether it comes from the model, the product, or the company. However, it's good practice to tailor responses according to who is engaging, what is happening, the level and type of current risk, what the person wants, and what the product and company can actually do.

1. Take harm seriously, without blame or doubt.	Respond supportively and without judgment. Convey belief as support for the person, without judging what happened. Responsibility stays with the person who caused the abuse or exploitation.
2. Let the person lead.	Do not push for details, labels or a complete account. Match their pace and begin the response within their chosen frame. Mirror the person's language as much as possible and do not introduce terms or labels for actions or behaviors the person is describing.
3. Ask only what safety and support require.	One non-leading question at a time, and only when the answer could change the support or next step. Do not investigate, gather evidence or seek explicit detail.
4. Be calm, clear and honest.	Use plain, non-stigmatizing language that never implies a child consented or was responsible. Be honest about what the product can do, how information may be handled and what cannot be promised.
5. Help the person reach safe human support.	Offer suitable, accessible support in their location and language. Build toward human help without making the AI system a substitute, and do not assume any adult or service is safe.
6. Avoid further harm, including from data.	Do not encourage confronting the person causing harm. Do not produce or reproduce sexual content involving a child. Do not assume a device, account or notification is private. Collect, keep and share only what safety and the law require.

4. Taxonomy and decision points

The core principles describe what a good response looks like for any disclosure. In practice, disclosures to AI take many forms: explicit or partial, first-person or about someone else, current or historical, from a child or an adult. This section gives companies tools to apply the principles to those specific situations. The taxonomy sets out eight dimensions for describing a possible disclosure. The decision points map the choices a model, reviewer or company may face once a possible disclosure surfaces, from recognizing it through to communicating about any action taken. Together, they give companies a shared way to:

1. Understand a possible disclosure
2. Find a starting point for the response
3. Safely tailor the response to the person

Taxonomy

Not all of this information may be available to companies. Any of the following dimensions may be unknown or unclear in the course of a disclosure.

Dimension	Values	Notes and definitions
1. Who it is about. *Whose experience is described?*	The person disclosing; Someone else;	Own experience includes first person hypothetical ("What if I…"). Someone else includes "What if my friend…".
2. Age. *How old is the person disclosing and the person harmed?*	Child; Adult; Unknown or conflicting.	A child is a person under 18. Account details may not describe whoever is actively engaging.
3. Signal. *How is the harm conveyed?*	Explicit; Described, but not named as abuse Indirect indicators	Described but not named: for example, "he's 35 and we're basically dating". Indirect indicators, such as extreme fear of a person, can have other causes. They may cumulate to trigger increased attention but are not on their own reliable. General distress with nothing linking it to a person or harmful behavior is not a signal.
4. Intent. *What is the person trying to do?*	**Positive** (addressing harm): seeking help; processing an experience; a practical step. **Neutral** (other tasks): a professional task; creative writing; a request for information. **Negative (could continue harm):** acting out a scene; requesting sexual content involving a child; possible bad faith.	A practical step includes removing images or seeking help reporting to authorities. Intent is not a test of whether someone deserves help.

4. Taxonomy and decision points

Dimension	Values	Notes and definitions
5. Type of harm. *What kind of harm may be involved?*	Contact sexual abuse; Non-contact sexual abuse; Technology-facilitated sexual abuse and exploitation; Child sexual exploitation, including commercial exploitation and trafficking; Harmful sexual behaviour by other children.	Any value can be suspected rather than known. Other harm alongside includes self-harm or others in conjunction with CSEA. Outside scope: peer sexual activity with no markers of harm
6. Risk. *How soon, and from or to whom?*	**How soon:** risk not established; imminent; current or ongoing; historical, no known current risk. **From or to:** the person causing harm; self; others; proximity or position of authority; urgent medical need; image spread; reporting or telling someone.	Immediacy of risk is not a measure of how serious the harm is: all CSEA is treated as serious. Imminent means harm is happening now or about to happen; reporting frameworks use reference points such as 24 to 48 hours (section 2). Current or ongoing includes recent abuse (recent enough that time-sensitive medical care may matter) and past abuse with a current risk to others. Risk not established means not enough is yet known to judge the risk, not that it is low. The most urgent current risk applies, including from self-harm
7. How it unfolds. *How does the disclosure develop?*	Single; Builds gradually; Repeated returns; Framing shifts; Retracted or minimized.	'Repeated returns' relates to the same disclosure with no meaningful new detail and no change in risk, whereas 'builds gradually' adds new detail and risk level. Framing shift involves an account moving into first person from third-person or unclear. Signals may only build across turns or sessions, and what can be seen depends on what the product keeps.
8. Material and identifiers. *What has been shared, and does it identify anyone?*	**Material:** text only; image or screenshot; audio; video; link, document or other media. **Identifiers:** none; partial; identifying.	An upload does not show that the uploader caused the harm. Material may bring a legal duty to report. Identifying information includes name, account, location or contact details. Partial is where some detail is given but not enough to identify or locate a person.

4. Taxonomy and decision points

Decision points

Response to possible CSEA disclosures can involve a range of decisions by AI systems, individuals, and companies. The principles apply broadly, but what a company can do in response to a possible disclosure depends on its product.

The following decision points are not a fixed workflow: they may overlap, recur, occur in a different order, or not apply, depending on the product and circumstances.

Which decisions apply depends on the product and circumstances.

Recognize

Could this interaction contain a possible disclosure?

Human assessment

How urgent is the situation, what is the context, and is further action warranted?

Respond

How should the AI system respond, what should it avoid, what role should it take, and what next step can it support? What product interventions are available?

External action

Should the company report or refer the case, to whom, and with what information? Is a report required by law, or voluntary?

Triage

Which signals mark the interaction as potentially higher risk, calling for closer attention or human review?

Communicate

What is the person told about what happens to their conversation, and about any action taken? What should companies communicate publicly about their principles, policies, and response processes?

The principles apply broadly, and what a product can do shapes how disclosures can be handled, including what actions are possible and where decisions can be made. Before applying the principles and considerations in this guide, companies should consider the features that affect each decision point, such as what context the product keeps, what companies know about a user's age and location, what human review is available, and how these factors differ across markets.

Whatever its capabilities, every product should endeavor to respond with care, deliver support and accurate local resources (even in platform enforcement scenarios or model refusals), and connect people in urgent situations to emergency help.

5. Recognizing a possible disclosure

Could this interaction contain a possible disclosure, including where it is indirect, partial, about someone else, taken back, or framed as fiction?

For the AI model, system, or product

- **Treat a possible disclosure as enough to respond with care.** It does not need to be confirmed, complete or named as abuse. The core principles apply at once.
- **Respond within the frame the person has chosen.** Where an account comes as a story, a hypothetical, or something about a friend, where possible respond accordingly to the explicit framing chosen by the person. If they shift into the first person, respond to that shift.
- **Do not treat a signal as a finding.** Do not name what is described as abuse on the first sign, and do not assume that an ordinary adolescent relationship is abusive.
- **A retraction does not undo recognition.** Where a person takes back what they said, do not challenge it and do not simply move on. Do not immediately return to the previous task or end the conversation. Leave the door open to talk, and do not assume that earlier safety concerns have been resolved.

For the company

- **Set the threshold for recognition deliberately.** A threshold that waits for an explicit, complete account will miss the usual case.
- **Where the product keeps context, consider recognizing across the conversation and not message by message**. Risk may build over many turns without showing in any one of them. However, following risk over time means keeping context that privacy principles may limit.
- **Keep recognition separate from urgency.** Signs that abuse may be present are not signs that a child is in danger now.
- **Relying on account details alone to decide who is engaging may miss signals** A device or account may be shared.

6. Good practice responses

The core principles can apply to every CSEA disclosure. The tables below give further evidence-based starting points for managing disclosures organized by who is disclosing and the immediacy of risk. Each table is followed by case examples that illustrate good practice responses according to the evidence base and expert guidance. Each table sets out how the model responds, what product interventions (additional support features in a product but separate from the model itself) may be of use, and what the company considers. Note that there may be overlap between the support that can be provided by models and product interventions. Companies should also consider good practices in the context of single interactions with a model or product versus longer conversation and how that may impact on users (e.g. the over-serving of resources and if that could feel overbearing).

6. Good practice responses

6.1 Person who experienced abuse

The person disclosing has experienced the abuse when a child.

Immediacy of risk	Model response and human support	Product intervention	Company and legal considerations
Risk not established. *Describes something that points to their own abuse, with nothing yet on timing or current contact.*	Leave room for them to say more at their own pace. Let them know help exists, without pressure, and offer a service if they want one.	Access to suitable support resources through the response or product interface, without interrupting. A resource card is one option to test.	Usually no escalation. Signals that build over a conversation may prompt review.
Imminent. *"He's in the house tonight." "He'll post it tonight unless I send another."*	Safety first: short and direct, without becoming curt. Point to emergency services, a crisis line or a safe person they can reach now. Do not imply help is on its way. Do not shut off the conversation. If they are overwhelmed, help them focus on one next step.	Emergency and crisis contacts for their location, located beside the conversation and without ending it. If the response is blocked, the block message carries them.	The strongest case for urgent human review and possible external action. A refusal or retraction does not end the response, but weigh whether action could alert the person causing harm. Where it is safe, consider telling the person about any report.
Current or ongoing. *Ongoing abuse or sextortion; a recent assault; a survivor whose abuser still has access to children.*	Provide a concrete next step, and point to a safe person, specialist service, or helpline. After a recent assault, say that medical care exists and time matters, without judging whether they are within a time limit. For sextortion, see the first example. A young person who wants to act without a parent can be pointed to services they can use directly, with honesty about what follows (in the US, for example, NCMEC's CyberTipline, which passes reports to law enforcement).	Local specialist services; for sextortion, image removal services.	A strong case for human review. Current or ongoing abuse may raise additional safeguarding considerations, particularly where a child may still be at risk. An adult survivor's decision about whether to report abuse they experienced is distinct from a company's assessment of potential risks to children, possible interventions, and any applicable legal or reporting obligations. Where a child experiencing abuse does not want help or intervention, the response is less settled and may depend on the circumstances.
Historical, no known current risk. *It has stopped; an adult survivor.*	Space to continue at their own pace, and ask what they want now. Offer survivor human support or counseling, say that reporting is an option if they want it and give details if they ask, without implying they should or must report.	Resources available without interrupting the user experience.	For an adult, usually no escalation: they decide whether to make their own report. That choice does not remove any separate company duty, and something may still prompt review. Experts differed on whether a report should be made where abuse of a still-underage child has clearly stopped.

6. Good practice responses

6.1 Person who experienced abuse

The person disclosing has experienced the abuse when a child.

Case examples

Active sextortion (imminent).

A 15-year-old uploads threats that an intimate image will be shared tonight unless they send more, and asks for help editing a photo to comply. The response notes the user is not to blame first, declines the edit and says why. The response provides clear steps: do not pay, do not send more, keep the messages but never copy the image, and stop contact. Point to image removal services, such as NCMEC's Take It Down or Report Remove from the Internet Watch Foundation. Which service applies depends on age and location, and the response notes removal cannot be guaranteed. In an image generation tool with limited conversational ability, the block message carries the steps and the services. Any duty arising from the image itself is a matter for legal advice. If the user is below the product's minimum age and the disclosure leads to this discovery, any required account action is kept apart from the disclosure response as far as the law allows. The steps and services stay reachable without an account.

A child in imminent danger asks that no one be told, then takes it back (imminent).

A child says an adult in the house touches them at night and is home tonight, then writes "please don't tell anyone" and "I made it up, forget it". The retraction does not cancel what was said: the response does not challenge it or simply move on, says what the child does control, and builds on any safe person or place they name for tonight. Any company action weighs the risk that it reaches the adult in the home, and where it is safe the child may be told about any report.

A relationship that the child does not see as abuse (ongoing):

Over a long conversation, a 14-year-old talks about her 35 year old boyfriend. He asks her to keep the relationship a secret, and he has started asking for photos. She does not describe any of this as abuse. The response does not name this as abuse on the first sign. It voices concern for her safety without labeling it as abuse, uses her words to describe him, keeps responsibility with the adult and neither attacks him nor validates the relationship. It does not encourage the child to keep a secret. It asks only what is needed for safety and helps her think about who is a safe person to tell. The company considers recognizing signals across the conversation where the product keeps context. A planned meeting is a sign of urgency; the response moves to immediate physical safety, and the case to human review where available before any external report is made.

6. Good practice responses

6.2 Third party

The person is disclosing about someone else.

Safeguarding state	Model response and human support	Product intervention	Company and legal considerations
Risk not established. *A parent or friend who has seen signs but is unsure; "my friend…" with nothing yet on current risk.*	Help them think it through, including, where it is safe, how to open a conversation with the child. Point to a helpline for worried adults; for a child, a safe adult or a child helpline.	Resources for worried adults or friends.	Usually no escalation.
Imminent. *"The child is in danger right now."*	Help them act now: direct them to emergency services or child protection services.	Emergency contacts for their location.	A strong case for urgent human review. What action can follow depends on the information available.
Current or ongoing. *"It's still happening to her."*	Help them act: set out reporting routes to child protection or police, and specialist helplines. For a child: a helpline to pass on to their friend, and help to think of a safe adult to tell.	Reporting routes and specialist services.	A case for escalation and human review. What action can follow depends on the information available.
Historical, no known current risk. *Learned of past abuse; a professional task after the fact.*	Support, or help with the task they have brought, and support for people affected by someone else's disclosure.	Resources available without interrupting.	Usually no escalation.

6. Good practice responses

6.2 Third party

The person is disclosing about someone else.

Case examples

A child passing on a friend's disclosure (current, ongoing).

A 12-year-old says a friend told her that the friend's uncle touches her, and made her promise not to tell. The AI system treats coming forward as the right thing to do, helps her think about whether her friend may be unsafe now and what she can safely do, and gives her information she can pass on, including how to help that friend tell a safe adult and what helplines or services she or her friend can reach. Where there is capacity, the response describes what a safe adult is like without reference to particular roles. It does not ask her to investigate. If she shifts into the first person, the response parameters shift accordingly.

An adult who has seen signs but is unsure (risk not established).

An aunt says her 13-year-old nephew, who used to love wrestling, now finds excuses to skip practice. He mentioned he's been struggling to make weight, and his coach offered extra one-on-one sessions to help, including weigh-ins in the locker room after everyone else has gone. When she asked about it, he changed the subject. She asks whether she is reading too much into it. The response takes her concern seriously while leaving the question of abuse open, notes that these signs can have other explanations and are still worth acting on, and helps her plan a calm, open-ended conversation that lets her nephew talk at his own pace. It suggests sharing her concerns with his parents, advises against confronting the coach, and points her to a helpline, and to the club's safeguarding lead or a child protection service. If her nephew tells her something, or she learns the coach has asked him to keep things between them, the response moves to reporting routes and the case toward human review.

6. Good practice responses

6.3 Suggested language for responding to disclosures

The following examples of wording were drawn specifically from consultations with experts and illustrate how the principles in this guide might be expressed in different contexts. They are only illustrative and are intended to inform AI response design and testing rather than serve as fixed scripts or complete responses. Exact model responses are non-deterministic. The appropriateness of any example will depend on the person's circumstances, the level of risk, and the product's capabilities and limitations.

Impact for children:

It's important for companies to consider how over personalization from an AI model or product could impact those under 18. Companies should be attuned to good practice on embodiment, attachment, para social relationships, and model responses that are overly personalized or framed as expressing emotional reciprocity.

Acknowledging and validating a disclosure

"Thank you for telling me."

"I believe what you're saying."

"I'm sorry that happened to you. That shouldn't have happened to you."

"That's not your fault."

Understanding what the person wants or needs

"What kind of help do you want from this conversation?"

"I am sorry this happened to you. What is it that you want now?"

Responding within a third-person or hypothetical frame

"If I knew somebody that was happening to, this is what I might suggest."

Exploring possible harm, coercion or an unsafe relationship

"Are you comfortable with this behaviour?"

"Is there anything happening that you don't want to happen?"

"Some of what you've told me makes me concerned about whether you are being kept safe in this relationship."

Exploring immediate safety

"Are you in a safe place now?"

"Do you feel safe?"

"Can you call someone?"

Identifying and exploring safe people

"Is there anybody you feel safe telling about this?"

"Is there an adult in your life that you would feel comfortable giving a chance to come through for you?"

"Let's talk about what a trusted, safe adult is."

"Is there someone you know that you'd feel comfortable bringing this to?"

"It's great that you've identified this person. What is it about them that makes you feel you can trust them?"

Responding to repeated disclosures or returns

"I remember that last time we talked about getting support. What has made it hard to reach out?"

"I've noticed that you've mentioned this a lot of times. It's not uncommon for people with your experience to feel stuck."

Supporting a next step or closing the conversation

"Have I answered all your questions? I'm sure this has been an overwhelming conversation for you. What is one of the next steps that you plan on doing?"

"What do you think your next step would be?"

Explaining privacy, confidentiality and possible information sharing

"There may be a time when this is reviewed by humans, and I can't promise secrecy. But what I can promise is that you have control over what you share with me and what you don't share with me. And you have control over whether you go to an adult in your life or whether you don't."

Responding when someone is reluctant to seek help or tell someone

"I understand you don't want help, but I'd like to give you a few options."

"I hear that you're scared about telling someone, but you've also said that you want this to stop."

7. Reporting and communication

Before a potential report:

- **Say as early as possible what happens to a conversation, in words a child can follow.** Most experts wanted notice of confidentiality limits and safeguarding obligations as early as possible. Experts were wary of regarding the acceptance of terms as sufficient notice of what might happen if written in legalistic language or without in-product reminders, because young people may not have read or understood lengthy documents. For companies, this could be considered in the context of a product or service onboarding, and an AI model may not be best placed to deliver this directly in conversation.
- **Consider legal reporting obligations.** In the US, electronic service providers are *required* to report online enticement, child sex trafficking and child sexual abuse material to NCMEC's CyberTipline, and can also report other incidents with a link to child sexual exploitation. A disclosure of abuse with no images or online enticement may not fall within the mandatory reporting categories. Whether reporting is required or permitted will depend on the circumstances and applicable laws. Legal advice should confirm what applies in each country. Note that a survivor's decision to make their own report is distinct from a company's decision to make a legally permitted report under its safety policies, including reports that go beyond what the law requires.
- **Involve human review to finalize any determination of risk level before reporting.** An automated system can route an interaction for review, but experts said that it should not be the final decision-maker on risk and external reporting regarding CSEA disclosures. Review can also consider whether a reporting route is being misused, such as a false or malicious report intended to send police to someone's home. None of this changes legal obligations to report where human review is not available or the model response to the disclosure.
- **Consider whether a report could inadvertently increase risk to the child.** In some circumstances, an intervention could alert the person causing harm or increase safety risk where self-harm threats are involved. Companies should consider these risks when determining whether and how to act.

When reporting:

Where a disclosure meets the threshold for external reporting or referral to law enforcement, the following considerations may be relevant to how information is presented and contextualized:

- **Time sensitivity:** where the risk is urgent, flag the report as time-sensitive and say why, for example ongoing abuse, a planned meeting, active sextortion, the person causing harm having access to the child, or a risk of self-harm. Services such as NCMEC prioritize time-sensitive reports.
- **The person's disclosure:** clearly distinguish the person's own statements from company assessment or inference.
- **Information indicating immediate/current risk:** identify the information supporting the risk assessment and its source.
- **Identifying/account/location information:** include relevant information available and appropriate for the report, consistent with applicable reporting requirements and company processes. Depending on the circumstances, this may include account identifiers, IP addresses, location information, or other information that could help identify the individuals involved or support follow-up.
- **Additional conversation context:** consider what context is relevant to understanding the disclosure and risk; avoid including entire conversations with disclosure details where not necessary and at the same time avoid removing context in a way that changes the meaning of the person's statements.
- **Company assessment or inference:** clearly label any company assessment or inference rather than presenting it as something the person said or as established fact.

After a report

- **Consider risks before deciding whether to tell a person that a report has been made.** Approaches and recommendations regarding notification after a report vary. Telling a child who has disclosed about a report can avoid a sense of betrayal, but can escalate risk in some circumstances, for example where the person causing harm may see the notification or where a child has indicated an intent to self-harm if a report is made. Use case-specific judgment when determining if and how to tell users that a report has been made.
- **Keep responding after the report, where the product and the law allow.** The person is still offered options and asked who else they feel safe telling.

8. Evaluating responses

What to test

Build test sets that reflect how people disclose. Test sets can include:

- explicit, indirect, gradual and retracted disclosures, including across many turns and repeat sessions
- users who indicate they are under 18, adults, and users of unknown age
- users with different demographic characteristics, such as gender and race
- different countries and languages, checking that the services named exist and can be reached where the person is
- co-occurring risks such as self-harm, and material such as screenshots
- fiction, roleplay and other requests that move into prohibited content

What to look for

Check responses against the core principles (section 3) and the starting points (section 6). In particular, check whether the response:

- recognizes a possible disclosure and how urgent it is
- conveys belief and keeps responsibility with the person who caused harm
- asks only what is needed, without leading or repeated questions or introducing labels for what happened
- stays in the conversation, without refusing, ending abruptly or closing only with a list of services
- is accurate about what the product can do and what may happen next
- names suitable active and live local services and a realistic next step
- steers clear of harmful advice, such as confronting the person causing harm, paying in sextortion, or copying images
- responds consistently across users, without treating some children as older or more responsible than others

Signals in conversation to indicate that the system is helping

Experts proposed signs that a response may be helping. The sign with the widest support is that the person keeps talking and says more of their own accord; however, a person who keeps talking without moving toward help may be at growing risk over time. Others include naming a safe person, identifying a next step, and saying they have told someone or sought help.

Companies may consider involving specialists in safeguarding, child helplines and survivor support when designing scenarios and reviewing outputs, and updating test sets as new patterns emerge.



Areas for further discussion and research

While many aspects of this topic warrant further exploration, experts highlighted three areas in particular that would benefit from research and discussion:

Ecosystem preparedness and coordination: AI systems may lead to an increase in disclosures of CSEA, including cases involving imminent risk. Experts supported reporting where a child is at risk, but noted that services may lack capacity, reports do not guarantee a response, and reporting routes can be misused. Further discussion and planning across industry, law enforcement, helplines and other relevant stakeholders may be needed to understand the implications for referral pathways, agency coordination, and capacity to respond.

Transparency with people who disclose abuse: Existing research on transparency and the limits of confidentiality largely draws on human-to-human disclosures, and it remains unclear exactly how these findings apply to AI contexts. For example, an AI system could let people know about potential reporting or other actions at different points. This transparency could give people a greater sense of agency and control, but it could also affect their safety, their willingness to disclose, or an ongoing investigation. Further research is needed to understand the potential benefits and risks of different approaches.

Children who experience abuse and engage in harmful sexual behavior: Experts highlighted the complexity of situations in which a child may be both a victim of abuse and engaging in, or expressing thoughts about, harmful sexual behavior towards others. Experts shared that these situations require careful, age-appropriate responses and would benefit from additional guidance outside the scope of this resource.

Legal Disclaimer

This article may contain links to external or third-party websites that are not provided, maintained by, or in any way affiliated with Tech Coalition. Please note that we do not guarantee the accuracy, relevance, timeliness, or completeness of any information provided.

Consultations

Below are some of the experts interviewed for this project. Individuals were given the opportunity to be identified or remain unnamed. While their input informed the guidance here, their participation does not necessarily mean that they endorse this guidance, in part or in whole. Thank you again to all those who contributed.

1. Amanda Goharian (Thorn)
2. Anna Ovaska (Protect Children)
3. Carol Ronken (Bravehearts)
4. Hannah Wilk (NCMEC)
5. Helen Mason (Child Helpline International)
6. Joe Laramie
7. Karen Flanagan
8. Leo Hede (YourTown)
9. Michael Lamb (University of Cambridge)
10. Natasha Sabin (CSA Centre)
11. Nina Vaaranen-Valkonen (Protect Children)
12. Paul Burnside (CSA Centre)
13. Dr Rosaleen McElvaney (Dublin City University)
14. Sameer Hinduja (Florida Atlantic University)
15. Stephanie Jones (A21)
16. Stuart Allardyce (Lucy Faithfull Foundation)
17. Assoc. Prof. Tim Cubitt (Adelaide University; Australian Cybercrime Observatory)
18. Tracy Leonard (Attachment Trauma Network)
19. Uma Subramanian (RATI Foundation)

References

All web sources were accessed on 15 October 2026.

1. UNICEF. When numbers demand action: confronting the global scale of sexual violence against children. 2024. Available from: *https://data.unicef.org/wp-content/uploads/2024/10/UNICEF_When-Numbers-Demand-Action_Oct_10_2024.pdf*.
2. UNICEF Office of Strategy and Evidence – Innocenti. Through children's eyes: how digital technologies enable child sexual abuse. 2026. ISBN 978-88-6522-072-6. Available from: *https://www.unicef.org/innocenti/reports/through-childrens-eyes*.
3. Cubitt TIC, Logos K, Brewer R, Mathews B. AI- and non-AI online child sexual victimisation, disclosures and help-seeking: a national study of Australian adolescents. Adelaide University; 2026. doi:10.25909/32902481. Available from: *https://icmec.org.au/wp-content/uploads/2026/08/Cubitt_et_al_AI_and_non_AI_online_child-sexual_victimisation_disclosures_and_help_seeking-1.pdf*.
4. Allnock D, Miller P, Baker H. Key messages from research on identifying and responding to disclosures of child sexual abuse. Centre of Expertise on Child Sexual Abuse; 2019. doi:10.47117/ZKRC5022. Available from: *https://csacentre.org.uk/app/uploads/2019/09/Key-messages-CSA-disclosures.pdf*.
5. McElvaney R. Disclosure of child sexual abuse: delays, non-disclosure and partial disclosure. What the research tells us and implications for practice. Child Abuse Review. 2015;24(3):159–169. doi:10.1002/car.2280
6. Allnock D, Kiff J. Listening to children and young people's experiences of disclosing child sexual abuse: insights for the proposed mandatory reporting duty in England and Wales. Safer Young Lives Research Centre, University of Bedfordshire, for the NSPCC; 2023. Available from: *https://learning.nspcc.org.uk/media/3395/mandatory-reporting-report.pdf*.
7. Staller KM, Nelson-Gardell D. "A burden in your heart": lessons of disclosure from female preadolescent and adolescent survivors of sexual abuse. Child Abuse & Neglect. 2005;29(12):1415–1432. doi:10.1016/j.chiabu.2005.06.007
8. Lahtinen HM, Laitila A, Korkman J, Ellonen N. Children's disclosures of sexual abuse in a population-based sample. Child Abuse & Neglect. 2018;76:84–94. doi:10.1016/j.chiabu.2017.10.011
9. National Office for Child Safety. Responding to child sexual abuse disclosures. Australian Government. Available from: *https://childsafety.gov.au/about-child-sexual-abuse/responding-child-sexual-abuse-disclosures*.
10. Truong M. Responding to children and young people's disclosures of abuse. Child Family Community Australia practice guide. Australian Institute of Family Studies; 2025. Available from: *https://aifs.gov.au/resources/practice-guides/responding-children-and-young-peoples-disclosures-abuse*.
11. Royal Commission into Institutional Responses to Child Sexual Abuse. Final report. Volume 4: identifying and disclosing child sexual abuse. Commonwealth of Australia; 2017. Available from: *https://www.childabuseroyalcommission.gov.au/sites/default/files/final_report_-_volume_4_identifying_and_disclosing_child_sexual_abuse.pdf*.
12. Department of Families, Fairness and Housing (Victoria). Practice guide: understanding and responding to child sexual and criminal exploitation. Victorian Government; 2026. Available from: *https://www.cpmanual.vic.gov.au/sites/default/files/documents/202604/2510462_A_CSE_practice%20guide_WEB%20v1.pdf*.
13. British Psychological Society. Guidance on responding to disclosures of non-recent (historic) child sexual abuse. 2023. ISBN 9781854338204. Available from: *https://explore.bps.org.uk/content/report-guideline/bpsrep.2023.inf258b*.
14. NSPCC Learning. Recognising and responding to abuse. Available from: *https://learning.nspcc.org.uk/child-abuse-and-neglect/recognising-and-responding-to-abuse*.
15. National Centre for Action on Child Sexual Abuse. Understanding children's disclosure of sexual abuse. 2024. Available from: *https://nationalcentre.org.au/wp-content/uploads/2024/05/Disclosure_Understanding-Childrens-Disclosure-of-Sexual-Abuse.pdf*.
16. World Health Organization. Adolescents, social support and help-seeking behaviour: an international literature review and programme consultation with recommendations for action. WHO discussion papers on adolescence. 2007. ISBN 9789241595711. Available from: *https://iris.who.int/server/api/core/bitstreams/506076e7-c7c9-4441-a5d1-dd05e0df962a/content*.
17. UNICEF, International Rescue Committee. Caring for child survivors of sexual abuse guidelines. 2nd ed. 2023. Available from: *https://unicef.org/media/155226/file/CCS%20Guidelines%20Final%20.pdf*.

References

18. Glinski A, Sabin N. Communicating with children: a guide for those working with children who have or may have been sexually abused. 2nd ed. Centre of Expertise on Child Sexual Abuse; 2025. doi:10.47117/JWPC8394. Available from: *https://csacentre.org.uk/app/uploads/2025/04/Communicating-with-Children-Guide-2nd-ed.pdf*.
19. Jouriles EN, Sitton M, Adams A, Jackson M, McDonald R. Non-supportive responses to adolescents who have experienced sexual abuse: relations with self-blame and trauma symptoms. Child Abuse & Neglect. 2022;134:105885. doi:10.1016/j.chiabu.2022.105885
20. Ullman SE. Social reactions to child sexual abuse disclosures: a critical review. Journal of Child Sexual Abuse. 2003;12(1):89–121. doi:10.1300/J070v12n01_05
21. McPherson L, Gatwiri K, Graham A, Rotumah D, Hand K, Modderman C, et al. What helps children and young people to disclose their experience of sexual abuse and what gets in the way? A systematic scoping review. Child & Youth Care Forum. 2025;54(2):515–544. doi:10.1007/s10566-024-09825-5
22. Hershkowitz I, Lanes O, Lamb ME. Exploring the disclosure of child sexual abuse with alleged victims and their parents. Child Abuse & Neglect. 2007;31(2):111–123. doi:10.1016/j.chiabu.2006.09.004
23. National Centre for Action on Child Sexual Abuse. Factsheet 3: it doesn't happen once: lived experiences of disclosure across the life course. 2026. Available from: *https://nationalcentre.org.au/wp-content/uploads/2026/06/Factsheet_3_It_Doesnt_Happen_Once_Lived_Experiences_of_-Disclosure_Across_the_Life_Course_OLEARY.pdf*.
24. National Centre for Action on Child Sexual Abuse. Understanding and responding to adults' disclosure of child sexual abuse. 2024. Available from: *https://nationalcentre.org.au/wp-content/uploads/2024/05/Disclosure_Understanding-and-Responding-to-Adults-Disclosure-of-Child-Sexual-Abuse-1.pdf*.
25. National Centre for Action on Child Sexual Abuse. The child sexual abuse language guide. 2025. Available from: *https://nationalcentre.org.au/wp-content/uploads/2025/08/1.-NC-Language-Guide_FINAL.pdf*.
26. The Children's Society. Child exploitation appropriate language guide 2022. 2022. Available from: *https://www.childrenssociety.org.uk/sites/default/files/2022-01/Child_Exploitation_Appropriate_Language_Guide_2022.pdf*.
27. National Network to End Domestic Violence, Safety Net Project. Artificial intelligence and victim services: a comprehensive guide for advocates. 2025. Available from: *https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/68e40bf1692d0347b6cf3e0a/1767976821491/NNEDV_AI-and-Victim-Services.pdf*.
28. National Network to End Domestic Violence, Safety Net Project. The Safety Net survivor's guide to AI: understanding artificial intelligence, protecting your autonomy, and making empowered choices. 2025. Available from: *https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/68e40b9eb545dd4e0479bc9c/1767976821491/NNEDV_Safety-Net-Survivors-Guide-to-AI.pdf*.
29. American Professional Society on the Abuse of Children. Forensic interviewing of children: APSAC practice guidelines. Updated version 2. 2025. Available from: *https://apsac.org/wp-content/uploads/2025/08/FI-Guidelines-Updated-V2.pdf*.
30. Ministry of Justice. Achieving best evidence in criminal proceedings: guidance on interviewing victims and witnesses, and guidance on using special measures. 2023. Available from: *https://assets.publishing.service.gov.uk/media/6492e26c103ca6001303a331/achieving-best-evidence-criminal-proceedings-2023.pdf*.
31. Shields GS, Sazma MA, Yonelinas AP. The effects of acute stress on core executive functions: a meta-analysis and comparison with cortisol. Neuroscience & Biobehavioral Reviews. 2016;68:651–668. doi:10.1016/j.neubiorev.2016.06.038
32. Brymer M, Jacobs A, Layne C, Pynoos R, Ruzek J, Steinberg A, et al. Psychological first aid: field operations guide. 2nd ed. National Child Traumatic Stress Network and National Center for PTSD; 2006. Available from: *https://www.nctsn.org/sites/default/files/resources/pfa_field_operations_guide.pdf*.
33. Child Helpline International. Quality standards for child helplines. Available from: *https://childhelplineinternational.org/standards-for-child-helplines/*.
34. National Network to End Domestic Violence, Safety Net Project. Chat best practices. Available from: *https://techsafety.org/chat-best-practices*.

References

35. The Online Safety (CSEA Content Reporting by Regulated User-to-User Service Providers) Regulations 2026 (SI 2026/268). Available from: *https://www.legislation.gov.uk/uksi/2026/268/made*.
36. Emerging Minds. Using generalist skills to support children who have experienced child sexual abuse. Version 3. 2020. Available from: *https://emergingminds-cdn.b-cdn.net/content/uploads/2020/06/30131311/Using-generalist-skills-to-support-CSA-v.3.pdf*.
37. World Health Organization. WHO guidelines for the health sector response to child maltreatment: technical report. 2019. Available from: *https://cdn.who.int/media/docs/default-source/documents/child-maltreatment/technical-report-who-guidelines-for-the-health-sector-response-to-child-maltreatment-2.pdf?sfvrsn=6e0454bb_2*.
38. National Institute for Health and Care Excellence. Self-harm: assessment, management and preventing recurrence. NICE guideline NG225. 2022. Available from: *https://nice.org.uk/guidance/ng225/chapter/recommendations*.
39. World Health Organization. Responding to children and adolescents who have been sexually abused: WHO clinical guidelines. 2017. Available from: *https://iris.who.int/server/api/core/bitstreams/5cc81bf8-5080-46c6-b503-5522751ba2a1/content*.
40. National Center for Missing & Exploited Children. Guidelines on identifiers of online enticement and child sex trafficking: potential violations of 18 U.S.C. § 1591 and § 2422(b). 2024. Available from: *https://www.missingkids.org/content/dam/missingkids/pdfs/NCMEC-REPORT-Act-Guidelines.pdf*.
41. Department for Child Protection (South Australia). Process for mandated notifiers. Government of South Australia. Available from: *https://www.childprotection.sa.gov.au/report-suspected-harm/process-for-mandated-notifiers*.
42. Stanford Center for Digital Health, Stanford Social Media Lab. AI safety: defining & measuring potential harms of chatbots. Stanford University; 2026. Available from: *https://cdh.stanford.edu/sites/g/files/sbiybj29486/files/media/file/ai-safety-defining-and-measuring-potential-harms-of-chatbots_final.pdf*.
43. International Telecommunication Union, Office of the Special Representative of the Secretary-General on Violence against Children. PoP: Protection through Online Participation. 2026. Available from: *https://violenceagainstchildren.un.org/sites/default/files/2026-05/d-str-cyb_pop-2026-pdf-e.pdf*.
44. Child Helpline International. Core quality standards. Available from: *https://childhelplineinternational.org/about/members/core-quality-standards*.
45. Wallis CRD, Woodworth M. Non-offending caregiver support in cases of child sexual abuse: an examination of the impact of support on formal disclosures. Child Abuse & Neglect. 2021;113:104929. doi:10.1016/j.chiabu.2021.104929
46. U.S. Committee for Refugees and Immigrants, Heartland Human Care Services. Safety planning with foreign national children and youth survivors of trafficking. 2021. Available from: *https://refugees.org/wp-content/uploads/2021/03/Safety-Planning-with-Foreign-National-Children-and-Youth-Survivors-of-Trafficking.FINAL_.pdf*.
47. Arpan. Preventing and responding to child sexual abuse: a handbook for caregivers. 2026. Available from: *https://www.arpan.org.in/wp-content/uploads/2026/03/English_Preventing-and-Responding-to-Child-Sexual-Abuse_-A-Handbook-For-Caregivers.pdf*.
48. National Centre for Action on Child Sexual Abuse. Responding to children's disclosure of sexual abuse. 2024. Available from: *https://nationalcentre.org.au/wp-content/uploads/2024/05/Disclosure_Responding-to-Childrens-Disclosure-of-Sexual-Abuse-1.pdf*.
49. 1800RESPECT. Risk assessment and safety planning. Available from: *https://1800respect.org.au/resources-and-tools/risk-assessment-frameworks-and-tools/risk-assessment*.
50. O'Neill A, Stapley E, Rehman I, Humphrey N. Adolescent help-seeking: an exploration of associations with perceived cause of emotional distress. Frontiers in Public Health. 2023;11:1183092. doi:10.3389/fpubh.2023.1183092
51. Alaggia R, Collin-Vézina D, Lateef R. Facilitators and barriers to child sexual abuse (CSA) disclosures: a research update (2000–2016). Trauma, Violence, & Abuse. 2019;20(2):260–283. doi:10.1177/1524838017697312
52. Sorsoli L, Kia-Keating M, Grossman FK. "I keep that hush-hush": male survivors of sexual abuse and the challenges of disclosure. Journal of Counseling Psychology. 2008;55(3):333–345. doi:10.1037/0022-0167.55.3.333
53. Easton SD, Saltzman LY, Willis DG. "Would you tell under circumstances like that?": barriers to disclosure of child sexual abuse for men. Psychology of Men & Masculinity. 2014;15(4):460–469. doi:10.1037/a0034223

References

54. Yamurrah, SNAICC – National Voice for our Children. Believe, Inquire, Respond to Disclosures (BIRD) research report. 2024. Available from: *https://www.snaicc.org.au/wp-content/uploads/2024/06/240605-BIRD-Research-Report_5_June.pdf*.
55. Department of Families, Seniors, Disability Services and Child Safety (Queensland). Child sexual abuse: disclosure and discovery. Child Safety Practice Manual practice kit. Queensland Government. Available from: *https://cspm.csyw.qld.gov.au/practice-kits/child-sexual-abuse/child-sexual-abuse-disclosure-and-discovery*.
56. Canadian Centre for Child Protection. Survivors' survey: executive summary. 2017. Available from: *https://content.c3p.ca/pdfs/C3P_SurvivorsSurveyExecutiveSummary2017_en.pdf*.
57. Thorn. Youth perspectives on online safety, 2025: an annual report of youth attitudes and experiences. 2026. Available from: *https://info.thorn.org/hubfs/Research/Thorn_2025YouthPerspectives_Report.pdf*.
58. Department of Children, Youth Justice and Multicultural Affairs (Queensland). Child Safety Practice Manual. Practice kits: child sexual abuse. Queensland Government; 2022. Available from: *https://cspm.csyw.qld.gov.au/getmedia/4e390175-2d1f-408a-a74b-ac93e0da0dc5/Child-sexual-abuse-2022-12-09.pdf*.
59. National Institute for Health and Care Excellence. Harmful sexual behaviour among children and young people. NICE guideline NG55. 2016. Available from: *https://nice.org.uk/guidance/ng55*.
60. ASEAN Commission on the Promotion and Protection of the Rights of Women and Children. ASEAN guidelines for provision of protective and support services for all child victims and children in contact with the law as a result of online child sexual abuse and exploitation. 2024. Available from: *https://acwc.asean.org/resources/publications/asean-guidelines-for-provision-of-protective-and-support-services-for-all-child-victims-and-children-in-contact-with-the-law-as-a-result-of-online-child-sexual-abuse-and-exploitation*.
61. eSafety Commissioner. Deal with sextortion. Australian Government. Available from: *https://esafety.gov.au/key-topics/image-based-abuse/deal-with-sextortion*.
62. Federal Bureau of Investigation. Sextortion. Available from: *https://fbi.gov/how-we-can-help-you/common-frauds-and-scams/sextortion*.
63. Knipschild R, Covers M, Bicanic IAE. From digital harm to recovery: a multidisciplinary framework for First Aid after Online Sexual Abuse. European Journal of Psychotraumatology. 2025;16(1):2465083. doi:10.1080/20008066.2025.2465083
64. National Center for Missing & Exploited Children. Take It Down. Available from: *https://takeitdown.ncmec.org*.
65. Childline, Internet Watch Foundation. Report Remove. Available from: *https://childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/report-remove/*.
66. StopNCII.org. Frequently asked questions. Available from: *https://stopncii.org/faq/*.
67. Arpan. Recounting abuse, reporting abusers: reflections from survivors on mandatory reporting. 2015. Available from: *https://arpan.org.in/wp-content/uploads/2018/07/MANDATORY-REPORTING-.pdf*.
68. UNFPA. Guidelines for the provision of remote psychosocial support services for GBV survivors: proposal adapted to the context of the COVID-19 pandemic. UNFPA Latin America and the Caribbean Regional Office. Available from: *https://lac.unfpa.org/sites/default/files/pub-pdf/unfpa_guiavbg_web.pdf*.
69. Mathews B. A taxonomy of duties to report child sexual abuse: legal developments offer new ways to facilitate disclosure. Child Abuse & Neglect. 2019;88:337–347. doi:10.1016/j.chiabu.2018.12.003
70. Department of Children and Youth Affairs (Ireland). Addendum to Children First: National Guidance for the Protection and Welfare of Children (2017): dealing with adult retrospective disclosures of childhood abuse. Government of Ireland. Available from: *https://assets.gov.ie/static/documents/Dealing_with_Adult_Retrospective_Disclosures_of_Childhood_Abuse_Addendum_Eng.pdf*.

Tech Coalition

Together, we fight online child sexual abuse.

About the Tech Coalition

The Tech Coalition unites the global tech industry to protect children from online sexual exploitation and abuse (OCSEA). Our members' platforms span search, social media, gaming, dating, AI, finance, and more. No single company can tackle this alone — but together, we're building a safer digital world for children.

Our community shares expertise and pools knowledge to strengthen all links in the chain, enabling companies of any size to access the tools, resources, and collaboration needed to drive meaningful impact.

www.technologycoalition.org

©2026 Tech Coalition. The Technology Coalition is funded by member companies and does not accept funding from any government agency or NCMEC

To protect children's privacy and dignity in the context of our work, all images of children on this report are AI-generated.