Your response

Question 1: To assist us in categorising responses, please provide a description of your organisation, service or interest in protection of children online.
Is this a confidential response? (select as appropriate) No
The National Center for Missing and Exploited Children (NCMEC) is a U.S.-based private, nonprofit organization founded almost 40 years ago to help find missing children, combat child sexual exploitation, and prevent child victimization. Today, NCMEC works globally to fulfill its mission through five main programs of work relating to: (1) missing children; (2) exploited children; (3) community outreach; (4) educational and professional resources; and (5) family support.

Question 2: Can you identify factors which might indicate that a service is likely to attract child users?
Is this a confidential response? (select as appropriate) No
Since 1998, NCMEC has operated the CyberTipline, the reporting mechanism for members of the public and electronic service providers (ESPs) to report instances of suspected child sexual exploitation. Over the past 25 years, NCMEC has handled more than 153 million CyberTipline reports submitted by thousands of ESPs and individual members of the public. Based on NCMEC's experience, we have found that a service is likely to attract child users based on its use of: • Platforms that incorporate features/graphics/animation/gaming targeted towards young audiences or specifically geared to children • Platforms that require parental/adult approval for young children to join or create an account • Platforms that incorporate an element of gamification (e.g., collecting jewels, points, reports, completing challenges) • Ability for a child to gain public-facing "likes" or followers • Ability for a child to share video content • Ability for a child to utilize features that enable chat/messages to disappear • Platforms that enable influencer culture by allowing youth to create content, be seen, and connect to each other and the world.

Question 3: What information do services have about the age of users on different platforms (including children)?

Is this a confidential response? (select as appropriate)

No

NCMEC does not have relevant information to provide in response to this question.

Question 4: How can services ensure that children cannot access a service, or a part of it?

Is this a confidential response? (select as appropriate)

No

NCMEC does not have specific relevant information to provide in response to this question, however several online platforms have incorporated various forms of age verification in order to ensure that children cannot access certain online services.

Question 5: What age assurance and age verification or related technologies are currently available to platforms to protect children from harmful content, and what is the impact and cost of using them?

Is this a confidential response? (select as appropriate)

No

Based on NCMEC's experience, Yoti (https://www.yoti.com/) is the most well-known third-party company used for age verification on online platforms. Some companies, such as Yubo, have utilized Yoti, as well as incorporated their own proprietary technology to conduct age verification of users on their platform. See https://www.yubo.live/blog/yubos-new-age-verification-feature-helps-keep-you-safe. Other companies have disclosed that they use a combination of human moderation and technology to conduct age verification. See https://onlyfans.com/transparency-center/verification ("How does OnlyFans seek to verify age and identity of Creators and Fans?")

Question 6: Can you provide any evidence relating to the presence of content that is harmful to children on user-to-user and search services?

Is this a confidential response? (select as appropriate)

No

The volume and severity of child sexual exploitation submitted to the CyberTipline over the past 25 years clearly establishes the proliferation of content that is inappropriate, criminal, and deeply harmful to children on a range of online platforms and services. NCMEC has compiled the following chart showing the number and type of reports relating to child sexual exploitation submitted to the CyberTipline in 2022:

2022 CyberTipline Reports by Reported Incident Type	
Child Pornography (possession, manufacture, and distribution)	31,901,234
Child Sex Tourism	940
Child Sex Trafficking	18,336
Child Sexual Molestation	12,906
Misleading Domain Name	1,948
Misleading Words or Digital Images on the Internet	7,517
Online Enticement of Children for Sexual Acts	80,524
Unsolicited Obscene Material Sent to a Child	35,624
Total	**32,059,029**

In NCMEC's experience, any online platform that enables users to interact and to share content can be used to sexually exploit a child. NCMEC has compiled the following chart showing the type of platforms involved in the 32,059,029 reports submitted to the CyberTipline in 2022:

Platform Type	**Count of Reports**
Adult Site	21,258
Chat or Messaging	23,425,960
Email	6,373
File Sharing	192,092
Forum or Message Board	58,990
Host or Provider	45,720
Hotline	81,168
Marketplace, Classified Advertising, or Payment	1,832
Online Gaming	8,540
Other	307
Safety Solutions (companies that offer moderation or monitoring services for other platforms)	36,866
Social Media	5,643,958

Question 6: Can you provide any evidence relating to the presence of content that is harmful to children on user-to-user and search services?

Umbrella Account (includes search engines)	2,279,461
Total	**31,802,525**

NCMEC also operates programs to support survivors who have been victimized by the re-circulation of CSAM depicting them online. These programs include notifying online platforms when they are hosting CSAM on a specific website or service. It is NCMEC's experience that despite receiving such notifications, CSAM is not uniformly removed or reported to NCMEC's CyberTipline but remains online and available to be viewed and shared.

Question 7: Can you provide any evidence relating to the impact on children from accessing content that is harmful to them?

Is this a confidential response? (select as appropriate)

No

NCMEC frequently receives requests from minors for help removing online sexually exploitative material in which they are depicted as well as reports submitted to the CyberTipline by minors who have been negatively impacted and harmed by exposure to online child sexual abuse material. As examples, the following are actual quotes from requests from minors for help removing online sexually exploitative content and from CyberTipline reports submitted by minors:

- "Unfortunately, videos were posted on the site without my consent during sexual activities. The friend who appears on the recordings is underage and has serious problems because of these films, me too....I believe this is psychological abuse, my friend is close to suicide...."
- "I found this link on [social media platform]...I clicked on the link...to my HORRIFYING discovery it was child porn...I cant get rid of the depictions. I would also like to include I'm a minor as well...."
- "There is clear child porn of ages even under 12...I was disgusted by the fact it existed...I am a 14 year old teenager and have been traumatized by the event...."

Question 8: How do services currently assess the risk of harm to children in the UK from content that is harmful to them?

Is this a confidential response? (select as appropriate)

No

NCMEC does not have relevant information to provide in response to this question.

Question 9: What are the exacerbating risk factors services do or should consider which may have an impact on the risk of harm to children in the UK?

Is this a confidential response? (select as appropriate)

No

All online platforms whether in the UK or elsewhere, should consider the following factors as potentially exacerbating risks for online child safety:

- Adoption of end-to-end encryption without child safety mitigating measures
- Failure to implement detection measures utilizing hashes, artificial intelligence, and machine learning across all platforms and services
- Failure to implement enhanced age verification methods on sites that may present additional risks for children (e.g., adult content sites, etc.)
- Failure to implement safety by design features when allowing minors to connect, especially on video chat platforms, with adults

Question 10: What are the governance, accountability and decision-making structures for child user and platform safety?

Is this a confidential response? (select as appropriate)

No

NCMEC does not have relevant information to provide in response to this question.

Question 11: What can providers of online services do to enhance the clarity and accessibility of terms of service and public policy statements for children (including children of different ages)?

Is this a confidential response? (select as appropriate)

No

It is important for online platforms to ensure that terms of service, including safety messaging, are easily accessible on various parts of their platform, written in age-appropriate language, and provided in multiple languages. Safety messaging should include clear guidance on how to report troubling content and users; how to reach out for additional resources in an emergency situation or when a user is in need of additional services; and how the online platform will respond to user reports and report back to users on resolution of complaints filed relating to online content.

Question 12: How do terms of service or public policy statements treat 'primary priority' and 'priority' harmful content?[1]

Is this a confidential response? (select as appropriate)

No

NCMEC does not have relevant information to provide in response to this question.

Question 13: What can providers of online services do to enhance children's accessibility and awareness of reporting and complaints mechanisms?

Is this a confidential response? (select as appropriate)

No

Online providers can take various steps to enhance children's accessibility to reporting and safety mechanisms when they are utilizing online sites, including the following:

- Providing in app reporting mechanisms
- Providing child-centered and survivor-informed safety policies
- Prominent publication of age-appropriate safety information
- Supporting and utilizing youth advisory councils

[1] See A1.2 to A1.3 of the call for evidence for more information on the indicative list of harms to children.

Question 14: Can you provide any evidence or information about the best practices for accurate reporting and/or complaints mechanisms in place for legal content that is harmful to children, or users who post this content, and how these processes are designed and maintained?

Is this a confidential response? (select as appropriate)

No

NCMEC is not aware of best practices relating to legal content that is harmful to children, but the following are 2 resources relating to the identification and reporting of illegal CSAM content:

- CSAM identification and reporting for US Companies (2022) (https://paragonn-cdn.nyc3.cdn.digitaloceanspaces.com/technologycoalition.org/uploads/CSAM-Identification_Reporting_R3-1.pdf)
- Technology Coalition industry classification system (https://paragonn-cdn.nyc3.cdn.digitaloceanspaces.com/technologycoalition.org/uploads/Tech_Coalition_Industry_Classification_System.pdf)

Question 15: What actions do or should services take in response to reports or complaints about online content harmful to children (including complaints from children)?

Is this a confidential response? (select as appropriate)

No

Companies should undertake a range of measures to ensure that they are handling reports relating to child sexual exploitation, including – and especially – reports from child victims and their families, appropriately. This range of measures would include:

- Providing in app reporting mechanisms
- Providing reporting mechanisms that are easily accessible and provide a feedback loop to the reporting person
- Enabling a reporting person to follow-up/track their report and receive referrals for additional services
- Promoting transparency regarding their public reporting
- Prominent publication of age-appropriate safety information and reporting processes

Question 16: What functionalities or features currently exist that are designed to prevent or mitigate the risk or impact of content that is harmful to children? A1.21 in the call for evidence provides some examples of functionalities.

Is this a confidential response? (select as appropriate)

No

NCMEC does not have relevant information to provide in response to this question.

Question 17: To what extent does or can a service adopt functionalities or features, designed to mitigate the risk or impact of content that is harmful to children on that service?

Is this a confidential response? (select as appropriate)

No

Please see response to Question 20.

Question 18: How can services support the safety and wellbeing of UK child users as regards to content that is harmful to them?

Is this a confidential response? (select as appropriate)

No

There are numerous measures that online platforms can implement to improve online child safety and to help ensure that child sexual exploitation is detected, reported, and removed from their services:

- Engage in voluntary hashing and grooming detection initiatives to enhance detection of suspected child sexual exploitation
- Adopt age verification and safety by design concepts that could reduce the exposure of children to harmful, including illegal, content
- Improve accessibility and ease of reporting disturbing content
- Limit the interaction of child users with adult users
- Blurring content that may be harmful/extreme. Some platforms are implementing measures that present a user with text/acknowledgment that material may be harmful and require a user to click to view the content

Question 19: With reference to content that is harmful to children, how can a service mitigate any risks to children posed by the design of algorithms that support the function of the service (e.g. search engines, or social and content recommender systems)?

Is this a confidential response? (select as appropriate)

No

NCMEC does not have specific expertise in this area, but online platforms can consider two mitigation strategies in this area:

- Limit or refrain from implementing algorithms into services that are accessible to and/or used by child users; and
- Apply safeguards and training parameters to any algorithms that are implemented in order to reduce the likelihood that an algorithm will connect a child with harmful and illegal content.

Question 20: Could improvements be made to content moderation to deliver greater protection for children, without unduly restricting user activity? If so, what?

Is this a confidential response? (select as appropriate)

No

Yes, virtually every online platform could improve child safety on their services by implementing additional content moderation practices. There are 2 primary measures that companies could adopt and implement across all of their platforms and services:

- Voluntary Hash Initiatives – NCMEC supports four hash-sharing initiatives to help ESPs that voluntarily elect to enhance their efforts to detect CSAM-related content on their platforms: (a) Non-Governmental Hash-Sharing Initiative – NCMEC shares over 13 million CSAM hashes (approximately 6.4 million NCMEC hashes and approximately 6.8 million hashes from other non-profits) with ESPs; (b) Exploitative Hash-Sharing Initiative – NCMEC shares over 300,000 hashes of sexually exploitative content that may not meet the U.S. legal definition of child pornography, with ESPs; (c) Industry Apparent Child Pornography Hash-Sharing Initiative – NCMEC facilitates ESP sharing of over 3 million apparent CSAM hashes with each other; and (d) Youth-Produced Imagery Hash-Sharing Initiative – NCMEC shares hashes submitted by minors of self-produced imagery in which the minors are depicted with ESPs. This initiative launched on December 30, 2022, and currently contains more than 8,000 hashes.
- Text/Enticement Detection Tools – Unlike hashing, the detection of enticement and sextortion crimes against children cannot be facilitated through hash

Question 20: Could improvements be made to content moderation to deliver greater protection for children, without unduly restricting user activity? If so, what?

initiatives. Instead, companies need to implement unique artificial intelligence and machine learning tools to detect these chat-based crimes against children.

Question 21: What automated, or partially automated, moderation systems are currently available (or in development) for content that is harmful to children?

Is this a confidential response? (select as appropriate)

No

NCMEC is aware of the following third party moderation systems that are available to detect child sexual exploitation content:

- CSAM detection of known content
  - Thorn's Safer Tool: https://safer.io/how-it-works/
  - PhotoDNA: https://www.microsoft.com/en-us/photodna
  - Shield (Canadian Centre): https://www.projectarachnid.ca/en/#shield
  - Google Content Safety API: https://protectingchildren.google/#tools-to-fight-csam
- Online grooming classifiers
  - Microsoft Project Artemis: https://blogs.microsoft.com/on-the-issues/2020/01/09/artemis-online-grooming-detection/
  - Thorn tool: https://www.ai
  - Thorn classifiers (https://www.ai.gov/rfi/2022/86-FR-56300/Thorn-Biometric-RFI-2022.pdf, pp. 2-3)

Question 22: How are human moderators used to identify and assess content that is harmful to children?

Is this a confidential response? (select as appropriate)

No

NCMEC does not have relevant information to provide in response to this question.

Question 23: What training and support is or should be provided to moderators?
Is this a confidential response? (select as appropriate) No
NCMEC does not have relevant information to provide in response to this question.

Question 24: How do human moderators and automated systems work together, and what is their relative scale? How should services guard against automation bias?
Is this a confidential response? (select as appropriate) No
NCMEC does not have relevant information to provide in response to this question.

Question 25: In what instances is content that is harmful to children, that is in contravention of terms and conditions, removed from a service or the part of a service that children can access?
Is this a confidential response? (select as appropriate) No
NCMEC does not have relevant information to provide in response to this question.

Question 26: What other mitigations do services currently have to protect children from harmful content?
Is this a confidential response? (select as appropriate) No
Several platforms have adopted child safety mitigation measures, including age verification, parental controls, default privacy settings for children, in-app reporting, and time limits for screen time (https://www.wired.co.uk/article/facebook-mute-push-notifications-app-dashboard). See, for example: Yubo:

Question 26: What other mitigations do services currently have to protect children from harmful content?
(https://www.yubo.live/blog/yubos-new-age-verification-feature-helps-keep-you-safe); Meta (https://about.fb.com/news/2023/01/providing-safe-experiences-for-teens/); TikTok (https://www.tiktok.com/safety/en-us/safety-privacy-controls/).

Question 27: Where children attempt to circumvent mitigations in place on a service, what further systems and processes can a service put in place to protect children?
Is this a confidential response? (select as appropriate) No
NCMEC does not have relevant information to provide in response to this question.

Question 28: Other than those covered above in this document (the call for evidence), are you aware of other measures available for mitigating the risk, and impact of, harm from content that is harmful to children?
Is this a confidential response? (select as appropriate) No
NCMEC does not have relevant information to provide in response to this question.