



TO: Ofcom

FROM: [Common Sense Media](#)

DATE: 20 October 2025

RE: [Consultation](#): Online Safety: Additional Safety Measures

CONFIDENTIALITY:

Per Ofcom's consultation response form, the whole response below is not confidential. Responses may be attributed to Common Sense Media.

Point of contact: Holly Grosshans, Senior Counsel, Tech Policy

RESPONSE:

Common Sense Media is dedicated to improving the lives of kids and families by providing the trustworthy information, education, and independent voice they need to thrive. Our ratings, research, and resources reach more than 150 million users worldwide, over 1.4 million educators, and more than 100,000 schools worldwide every year. Backed by the research that's the foundation of everything we do, we champion quality media that entertains and inspires, and support legislation that aims to close the digital divide and hold social media and AI platforms accountable for their effects on minors. We encourage students and educators to think critically about technology and become responsible digital citizens. And we safeguard children's health and well-being by protecting their data privacy and reducing potential online harms.

We are pleased to submit these comments in response to Ofcom's Consultation – Online Safety: Additional Safety Measures. Common Sense Media supports Ofcom's efforts to protect the safety of minors online while ensuring their freedom of expression. We offer constructive suggestions below to achieve this balance.

More specifically, our responses to the consultation:

- Highlight recent U.S. legislative actions and proposals aimed at reducing online harms affecting children.

QUESTION 6: Do you consider that there are alternative measures which would materially reduce the risks to users from livestreaming, such as preventive safety by design frictions, prompts, or restrictions? If so, please detail them and provide evidence on the costs and efficacy.

First, we commend Ofcom for taking tangible steps to encourage accountability among all online platforms for their effects on minors. Ofcom has commendably tackled a broad range of online threats to minors and admirably proposes to expand coverage to reduce continued online harm. Common Sense Media is a staunch advocate for legislation and regulations that limit the harm of unwanted contact by online strangers towards minors. See the New York Children’s Online Safety Act (“NY COSA”)¹, introduced during the 2025 legislative session, and also California’s Protecting Our Kids from Social Media Addiction Act (“Social Media Addiction Act”),² signed into law on September 20, 2024. Given Common Sense Media’s expertise in research and in policy advocacy concerning online harms to children, we support Ofcom’s expansion of its Codes of Practice as part of the Online Safety Act of 2023 for providers of one-to-many livestreaming products (i.e, social media platforms), and specifically affirm proposal ICU F3 as we believe it will effectively mitigate harms to children using and interacting with online livestreaming.

According to the UK nonprofit, National Society for the Prevention of Cruelty to Children (NSPCC), hosting and/or watching livestreams significantly increases the risk to kids of exposure to “inappropriate or upsetting content”³. While NSPCC defines this type of content as “sexual, abusive, violent content,”⁴ an October 2025 Common Sense Media study on boys in the digital world shows how exposure to even “digital masculinity” content, which includes messages about making money, building muscle, dating, fighting or weapons, being providers or protectors, and various gender stereotypes,” can have significant effects on young boys⁵. For instance, boys with heavy “digital masculinity” exposure have more negative self-esteem, are significantly more likely to suppress their emotions, avoid vulnerability, and are more likely to report being lonely⁶. This content is almost unavoidable, with over two-thirds of adolescent boys (69%) regularly seeing masculinity content that promotes problematic gender stereotypes.⁷ Parents of young boys face an uphill battle to counteract what they see online, as adolescent boys increasingly live and connect online, with 94% of them using social media or games daily⁸.

¹ S. 4609, 2025-2026 Leg., Reg. Sess. (N.Y. 2025); A. 6549, 2025-2026 Leg., Reg. Sess. (N.Y. 2025).

² Protecting Our Kids From Social Media Addiction Act, Cal. Health & Safety Code § 27000-07 (2024).

³ *Livestreaming and online video apps*, NSPCC, <https://www.nspcc.org.uk/keeping-children-safe/online-safety/livestreaming-online-video-apps/> (last visited Oct. 9, 2025).

⁴ *Id.*

⁵ MICHAEL B. ROBB & SUPREET MANN, *Boys in the Digital Wild: Online Culture, Identity, and Well-Being*, COMMON SENSE MEDIA (2025), <https://www.common Sense Media.org/sites/default/files/research/report/2025-boys-in-the-digital-wild-report-for-web.pdf>.

⁶ *Id.* at 2-4.

⁷ *Id.* at 2.

⁸ *Id.* at 7.

These issues have very real implications, as nearly half of boys believe they must follow "unwritten rules," like not crying or showing fear, to avoid being teased or picked on⁹.

Young boys aren't the only ones negatively affected by social media usage. A 2023 Common Sense Media report on girls' relationship with social media explains how roughly seven in ten susceptible young girls who use Instagram (75%) and TikTok (69%) say they come across problematic suicide related content at least monthly on these platforms¹⁰. Also, nearly half of adolescent girls of color report exposure to racist content or language on TikTok (48%) or Instagram (48%) at least monthly¹¹. Additionally, across platforms, LGBTQ+ adolescents are roughly twice as likely as non-LGBTQ+ adolescents to encounter hate speech related to sexual or gender identity¹². Children being exposed to harmful content online is not new; however, livestreaming adds new dangers that only exacerbate an already unsafe online world. The risk of exposure to this type of content explicitly increases as children engage with unmoderated streams and comment sections through one-to-many livestreaming products¹³.

The COVID-19 pandemic has also exacerbated children's adoption of social media¹⁴. Research into livestreaming habits among young people in 2017 found that one in ten 8 to 17-year-olds has gone live¹⁵. The NSPCC also conducted a survey in March 2018 of 40,000 young people between 7 and 16 and found that 24% of all children have delivered a livestream broadcast¹⁶. Research commissioned as part of Zurich's Safer Schools initially saw a 17% rise in livestreaming amongst children during the first lockdown, with more than one in five 'broadcasters' communicating with strangers online¹⁷. Common Sense's own report found that the majority of girls who use Instagram (58%) and Snapchat (57%) say they've been contacted by a stranger on these platforms in ways that make them uncomfortable¹⁸. Also, nearly half of girls who use TikTok (46%) have had this experience on the platform¹⁹.

⁹ ROBB & MANN, *supra* note 5, at 5.

¹⁰ JACQUELINE NESI, SUPREET MANN, & MICHAEL B. ROBB, *Teens and Mental Health: How Girls Really Feel About Social Media*, COMMON SENSE MEDIA (2023), https://www.commonsensemedia.org/sites/default/files/research/report/how-girls-really-feel-about-social-media-researchreport_web_final_2.pdf.

¹¹ *Id.* at 10 (susceptible young girls defined as "girls with moderate or severe depressive symptoms").

¹² *Id.* at 11.

¹³ *Id.* at 35; LORNA PONAMBALUM, *Livestreaming: What are the Online Risks for Children and Young People?*, THE NATIONAL COLLEGE, (Mar. 22, 2023), <https://nationalcollege.com/news/livestreaming-what-are-the-online-risks-for-children-and-young-people>.

¹⁴ VICTORIA RIDEOUT, ET. AL, *Coping With Covid-19: How Young People Use Digital Media to Manage Their Mental Health*, COMMON SENSE MEDIA (2021), <https://www.commonsensemedia.org/sites/default/files/research/report/2021-coping-with-covid19-full-report.pdf>.

¹⁵ PONAMBALUM, *supra* note 13.

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ NESI, MANN, & ROBB, *supra* note 9, at 15.

¹⁹ *Id.*

While Ofcom is no stranger to online harms for children, several other safety-by-design features and “friction” points, not included in proposal ICU F3, are available to mitigate these risks. The U.S. based non-profit Electronic Privacy Information Center (EPIC) uses the term “friction” to describe design elements that slow down user processes on social media²⁰. For example, there is an obvious concern that self-attestation, while easy, is an insufficiently accurate tool for age assurance. However, there is reason to believe that certain design features can enhance the effectiveness of self-attestation. To ensure more accurate age verification, a web service may require users to wait a certain amount of time before changing their birthdate upon joining, rather than allowing the change immediately after account creation. This feature deters children who might sign up for an app or platform with their correct age, but then later change their age to access the whole product.

According to Common Sense Media research, algorithms, not user intent, are the primary driver of boys' exposure to posts about masculinity²¹. 68% of boys who see material online say it started appearing in their feed without them searching for it²². Targeting these addictive features, especially for children, is a valuable tool for advocates. The Social Media NUDGE Act, a bill introduced but not passed in the U.S. Senate, tried to tackle these algorithmic issues²³. It sought to address the growing influence of behavioral design on users by identifying and restricting manipulative “nudge” features on social media platforms²⁴. These design elements, such as engagement-driven algorithms, infinite scroll, and targeted notifications, are often used to maximize user attention but can contribute to addiction, misinformation, and mental health harms²⁵. This act represents a broader policy effort to mitigate the social costs of engagement-based business models without imposing direct content regulation or infringing on free expression²⁶.

Proposal ICU F3 doesn't allow users, both other children and adults, to interact with children livestreaming, which is an excellent start to mitigating harms online. There are, however, additional design features or friction points that social media companies can implement to stop or slow down the use of livestreaming. For example, if a user under the age of 18 attempts to start a livestream, a prompt may pop up before they actually go live, giving the child a moment to pause and think. A prompt like, “Are you sure you want to go live?” along with an explanation of what that means, might stop a child from going live or even prevent an accidental livestream. Additionally, Ofcom could require platforms not to allow users under 18 to comment or gift during other people's livestreams. Requiring such design features could mitigate the risk of children interacting with strangers, especially adults, online.

²⁰ EPIC, Amicus Brief for NetChoice, LLC v. Rob Bonta, Attorney General of the State of California, in his official capacity, December 2023.

²¹ <https://cdn.sanity.io/files/3tzzh18d/production/c567c26dc66cd9839ab87ec6db9b95975d80b1c4.pdf>.

²² ROBB & MANN, *supra* note 5, at 8.

²³ *Id.*

²⁴ Nudge Act, S. 3608, 117th Cong. (2022), <http://www.congress.gov/bill/117th-congress/senate-bill/3608>.

²⁵ *Id.*

²⁶ *Id.*

QUESTION 13: Do you agree with the harms currently in scope of these measures? Are there any additional harms that these measures should capture? Please provide the underlying arguments and evidence that support your views, including evidence regarding the availability of accurate and effective proactive technology.

We again commend Ofcom for taking tangible steps to encourage accountability across all online platforms for their effects on minors, and specifically adding policy about proactive technology. Common Sense Media agrees with the harms currently in scope of Ofcom's proactive technology recommendations, especially the illegal harms that affect children, like CSAM, suicide encouragement, and fraud, and the primary-priority content (PPC) harmful to children, like suicide, self-harm, eating disorders, and pornography²⁷. It is well known that CSAM is extremely harmful, however, studies have also shown that possession and distribution of CSAM leads to other types of sexual exploitation of minors²⁸. The implementation of proactive technology through hash matching, URL matching, and certain classifiers already exists and is reasonably accurate, making the requirement for proactive measures here both technologically and legally justifiable²⁹.

However, there are additional harms and tools available to address the effects of these materials. For instance, the TAKE IT DOWN Act, which Common Sense Media endorsed, is the first significant bipartisan federal legislation to provide a baseline level of protection against the spread of non-consensual intimate imagery (NCII), including AI-generated deepfake pornography and so-called "revenge porn."³⁰ The Act amends the US Communications Act to criminalize the knowing publication of intimate visual depictions (real or AI-generated) without consent, and requires online platforms to implement rapid takedown mechanisms³¹. Victims can submit verified removal requests, and platforms must delete or disable access to the content within 48 hours, a statutory obligation that differs from Ofcom's recommendations³². It explicitly establishes federal protections against the online distribution of NCII and deepfakes, closing long-standing gaps in privacy and digital harm law by introducing explicit liability for both individual

²⁷ Ofcom, *Consultation: Additional Safety Measures* (U.K.) 76-77 (30 July 2025), <https://www.ofcom.org.uk/siteassets/resources/documents/consultations/.../consultation-additional-safety-measures-30-july-2025.pdf>.

²⁸ JANIS WOLAK, DAVID FINKELHOR & KIMBERLY J. MITCHELL, *Child Pornography Possessors Arrested in Internet-Related Crimes: Findings from the National Juvenile Online Victimization Study*, CRIMES AGAINST CHILDREN RESEARCH CTR. (2005), <https://scholars.unh.edu/ccrc/33/>.

²⁹ *An Update on Voluntary Detection of CSAM*, TECH COALITION, (Apr. 11, 2024), https://technologycoalition.org/resources/update-on-voluntary-detection-of-csam/?utm_source=chatgpt.com.

³⁰ COMMON SENSE MEDIA, *S. 146 TAKE IT DOWN Act Coalition Support Letter* (Apr. 9, 2025), <https://www.common sense media.org/sites/default/files/featured-content/files/s.146-take-it-down-act-coalition-support-letter-4.9.2025.pdf>; TAKE IT DOWN Act, S. 146, 119th Cong. (2025), <https://www.congress.gov/bill/119th-congress/senate-bill/146>.

³¹ TAKE IT DOWN Act, *supra* note 30.

³² ARAVIND SWAMINATHAN, ET. AL, *TAKE IT DOWN Act Becomes Law, Introducing Landmark Federal Protections to Combat Online Exploitation and Deepfakes*, ORRICK (May 21, 2025), <https://www.orrick.com/en/Insights/2025/05/TAKE-IT-DOWN-Act-Becomes-Law>.

offenders and non-compliant platforms³³. The legislation seeks to deter the spread of exploitative content and provide consistent, nationwide recourse for victims³⁴.

Another gap in Ofcom's recommendation is the lack of explicit mention of AI or deepfakes. There are several useful examples for Ofcom to accomplish this important policy. The state of California passed in 2024 the California CSAM AI Law (AB 1831), which protects children by modernizing the definition of "obscene matter" in existing California law to ensure that AI-generated child sexual abuse material (CSAM) is also illegal to possess or distribute³⁵. Previously, in California, prosecuting CSAM possession and distribution cases, prosecutors had to prove that the CSAM at issue depicts an actual child³⁶. However, with today's AI generating such realistic images, there is often no way to distinguish a deep fake from reality³⁷. Before this bill, people who possess CSAM depicting actual children could evade prosecution by claiming the images are AI-generated³⁸. Law enforcement officers in California have already encountered instances where people possess CSAM that might not be prosecuted because the images were generated by AI or because the officer could not prove the image was authentic³⁹. Under this law, CSAM offenders will be held accountable for possessing CSAM images, whether they depict an actual child being abused or if they are digitally altered images or images made with AI⁴⁰.

CONCLUSION:

In conclusion, Common Sense Media commends Ofcom for its ongoing leadership in advancing robust regulatory measures to protect children online. The proposed expansion of the Online Safety Act Codes of Practice represents an important step toward ensuring accountability across platforms and mitigating the unique risks posed by one-to-many livestreaming environments. Proposal ICU F3 is a significant advancement in limiting children's exposure to harmful interactions online, and its inclusion of proactive technological measures demonstrates an evidence-based approach to safeguarding minors. We respectfully recommend that Ofcom further strengthen these protections by incorporating additional safety-by-design requirements discussed above - such as friction-based prompts, enhanced age assurance mechanisms, and restrictions on interaction features - to more effectively deter exposure to harmful content and unwanted contact.

³³ TAKE IT DOWN Act, *supra* note 30.

³⁴ *Id.*

³⁵ COMMON SENSE MEDIA, *CA CSAM AI (Berman) Bill – One Pager* (June 2024), <https://www.common sense media.org/sites/default/files/featured-content/files/ca-csam-ai-berman-bill-one-pager-2024-updated-6.2024.pdf>.

³⁶ *Id.*

³⁷ *Id.*

³⁸ *Id.*

³⁹ Jon Healey, *Scandal Over AI-Generated Nudes at Beverly Hills Middle School Highlights Gaps in Law*, L.A. TIMES (Mar. 3, 2024, 7:34 AM), <https://www.latimes.com/california/story/2024-03-03/scandal-over-ai-generated-nudes-at-beverly-hills-middle-school-highlights-gaps-in-law>.

⁴⁰ *CA CSAM AI (Berman) Bill*, *supra* note 35.

Moreover, we encourage Ofcom to explicitly account for emerging forms of harm enabled by artificial intelligence, including AI-generated child sexual abuse material and non-consensual deepfake imagery. Incorporating these considerations would align the Online Safety Act's implementation with recent legislative developments in the United States, such as the TAKE IT DOWN Act and California's CSAM AI Law (AB 1831), which address parallel threats through modernized legal frameworks. By integrating these forward-looking measures, Ofcom can further solidify the United Kingdom's position as a global leader in promoting a safer and more accountable digital environment for children.

We appreciate the opportunity to participate in the Online Safety: Additional Safety Measures Consultation. As a trusted global brand dedicated to children and families, we are eager to contribute our perspectives as Ofcom formulates essential regulatory guidance, standards, and tools aimed at enhancing the well-being of children in the UK.

ABOUT COMMON SENSE MEDIA UK:

Common Sense Media is an independent nonprofit organisation dedicated to helping children thrive in a rapidly changing world. The organisation is based in San Francisco, California with regional offices across the U.S. Common Sense launched its first international office in the UK in 2019, a registered charity (also Common Sense Media, 1188840), through which it rates, educates, investigates, and advocates for the safety, privacy, and well-being of children in the UK and globally.

For more information, visit <https://www.commonsense.org/> and <https://www.common sense media.org.uk>