CHILD ONLINE HARMS POLICY THINK TANK

ICC
THE INSTITUTE FOR CONNECTED COMMUNITIES

University of East London
Pioneering Futures since 1898

The Child Online Harms Policy Think Tank Launch Report (18 June 2025)

Authors:
Professor Julia Davidson (OBE)
Ms Alexandra Deac
Ms Boglarka Meggyesfalvi
Dr Ruby Farr

Organisation:
Institute for Connected Communities, University of East London, Water Lane, London

Recommended citation: Davidson, J., Deac, A., Meggyesfalvi, B., & Farr, R. (2025). The Child Online Harms Policy Think Tank Report. Child Online Policy Think Tank, University of East London.

Contents

This report contains descriptions, summaries, experiences or allusions to topics that may be sensitive or that some people might find distressing, including:

- Online grooming
- Solicited and unsolicited sharing of sexual images
- Online harms
- Suicide ideation
- Self-harm

Use of trigger words warning

We appreciate that different people might experience the content of this report differently. That is why we recommend stopping reading if, at any point, you experience any type of distress or discomfort and seek support from professional bodies.

We provided a non-exhaustive list of key links below:

Organisation	Description/contact
ChildLine	0800 1111, chat online via www.childline.org.uk/get-support/1-2-1-counsellor-chat
Samaritans	Confidential listening service, available 24/7. Call 116 123, online at www.samaritans.org
NSPCC	0808 800 5000, online at emailing help@NSPCC.org.uk
Shout	Support during a mental health crisis 24/7, text SHOUT to 85258
Parents Helpline	0808 802 5544, or chat online via www.youngminds.org.uk
CEOP (Child Exploitation and Online Protection)	www.ceop.police.uk/Safety-Centre
Internet Watch Foundation (IWF)	If you've seen or been affected by indecent images or videos online, you can report them anonymously to the IWF. Report here: www.iwf.org.uk
Embrace Child Victims of Crime	03456099960, online at embracecvoc.org.uk
Papyrus (Prevention of Young Suicide for under 35)	800 068 4141, online at www.papyrus-uk.org
UK Safer Internet Centre	Advice and reporting of harmful content online at www.saferinternet.org.uk
In platform reporting	You can usually report inappropriate behaviour or exploitation directly within an online platform / social media app / the game itself. The process can differ depending on the platform or game you're using. Common Platforms: ■ Roblox: Click on the player's profile → Select "Report Abuse" → Choose the reason. ■ Fortnite: Menu → Reporting/Feedback → Report Player → Select reason. ■ PlayStation / Xbox: Access player's profile → Report → Choose category.

Executive Summary

Children’s increasing exposure to digital environments has intensified concerns about online harms. Ofcom’s latest data (2023) indicates that nearly 90% of children aged 3–4 now go online (as reported by parents), a substantial rise from 52% in 2018. The use of video-sharing platforms (VSPs) such as YouTube has also surged, from 45% in 2018 to 87% in 2023, raising serious questions about the appropriateness and safety of digital content targeting young users.

Despite platform age restrictions and moderation policies, harmful content remains easily accessible. Past research revealed that children could encounter explicit or violent material within just 2–4 clicks from child-friendly videos (Halliday, 2013). This issue persists today, with numerous media investigations exposing disturbing videos labelled with popular characters like “Elsa” or “Spiderman” that depict sexualised behaviour, violence, or vandalism, deliberately bypassing filters and exploiting recommendation algorithms.

The proliferation of such risks is further compounded by the rapid integration of Artificial Intelligence (AI) in digital services. AI-powered systems, such as algorithmic content feeds and Generative AI (GenAI) tools, can inadvertently or deliberately expose children to inappropriate content, encourage risky behaviours, and enable new forms of abuse, such as deepfakes or targeted exploitation. These harms are often amplified by business models that prioritise engagement and monetisation over safety, and by design features that exploit children’s developmental vulnerabilities.

In response, this report advocates for a proactive, evidence-based policy agenda that centres child rights and wellbeing in the design, governance, and regulation of digital platforms. Drawing on recent research, including findings from Ofcom, the VIRRAC project, and the CC-DRIVER initiative, it outlines the nature and scale of online harms, emerging threats posed by new technologies, and the structural gaps in current regulatory frameworks. The report concludes with concrete recommendations for policymakers, regulators, and industry stakeholders to embed safety-by-design, improve accountability, and ensure children can participate in digital life free from harm.

1. Introduction

1.1 Aims of this report

The Child Online Harms Policy Think Tank is an independent, academic initiative dedicated to informing and influencing policy on child online safety by leveraging a research evidence-based approach. Its work focuses on addressing the evolving risks posed by digitalisation and AI while advocating for children's digital rights and fostering collaboration among policymakers, academics, and stakeholders.

The Child Online Harms Policy Think Tank aims:

1. **To inform and influence policy on child online harms using a research evidence-based approach.** Using a research evidence-based approach, the Think Tank will critically review existing policies, including their ability to anticipate and address future risks associated with AI and digitalisation.
2. **To engage directly with policymakers to translate research findings into actionable policy.** The Think Tank will provide a bridge between academic research and policy in this area, drawing upon our research but also the work of other key academics in this area to inform policy.
3. **Identify research gaps in the online harms area, commission and undertake research in a timely manner to inform policy and practice with children and young people in the rapidly evolving digital landscape.**

Our strategic vision is based on the following pillars:

1. **Driven by impact** – we want to support impactful, real-life translation of research and policy into practical outputs that support child online safety.
2. **Interdisciplinarity** – we appreciate the value that multiple disciplines and perspectives bring, and we will engage with policymakers and other key stakeholders and colleagues, transposing fields and bridging academic research and policy.
3. **Involvement** – we will prioritise collaboration with a broad range of stakeholders, including policymakers, educators, parents and children to identify research gaps and to undertake timely research.

Our strategy puts well-being and online safety at the heart and purpose of our activities and endeavours. The Child Online Harms Policy Think Tank will act as an independent, central hub for research, policy development, and collaboration aimed at safeguarding children and young people in the digital age.

1.2 Digital childhood: context and trends

Children, defined under international law as anyone under 18 (OHCHR, 1989), are immersed in online environments from an early age, often without adequate safeguards. According to Ofcom (2023a), nearly 90% of children aged 3–4 now go online, up from 52% in 2018, and 95% of young people aged 3–17 use the internet daily (Ofcom, 2024). Access to mobile devices is near-universal, with 99% of children owning a mobile phone by age 11 (Ofcom, 2022a).

Despite age restrictions (typically 13+ years) on platforms like TikTok and Instagram, children are finding ways to gain access. In a qualitative study by Ofcom (Ofcom, 2022a), 35 out of 42 children reported using social media or video-sharing sites, with many admitting to falsifying their age, in some cases claiming to be over 50.

This widespread and unsupervised access coincides with a dramatic evolution in the types of content children engage with. The current digital landscape is increasingly shaped by short-form videos, livestreaming, algorithmically curated feeds, and AI-generated content. Platforms such as TikTok, YouTube Shorts, and Snapchat prioritise fast, engaging, and emotionally charged media, often without meaningful age filtering or moderation (Nagata et al., 2025).

Much of this content is amateur or user-generated, carrying risks of mislabelling, misinformation, or exposure to violent, sexual, or otherwise harmful material. For instance, children searching for popular characters like “Elsa” or “Spiderman” may encounter videos tagged for young viewers but featuring violent or explicit themes (Halliday, 2013).

This multifaceted engagement amplifies vulnerability. Without the developmental maturity or digital literacy to critically assess online content, and often without adult guidance, children are increasingly exposed to emotionally provocative, misleading, or harmful material.

1.3 Nature and scale of online harms

Children are particularly vulnerable to online risks, especially when content is not age- or stage-appropriate (NSPCC, 2024).

Ofcom reports two types of risk exposures among children (Ofcom, 2025f):

- **Isolated exposure:** Accidental encounters with violent, sexual, or otherwise harmful material.
- **Cumulative exposure:** Extended, repetitive engagement with potentially harmful themes (e.g., body image-focused content).

While not all risks necessarily lead to harm (Livingstone et al., 2017), certain factors, including vulnerability, age, gender, and offline circumstances, can increase the likelihood of harm (Davidson et al., 2021). The problem is not only widespread but also intensifying. The exposure to and use of technology among children has led to increased instances of child online harm. Risk of exposure is present across many different services, not limited to large or small platforms. For example, risk factors include business models prioritising revenue and engagement over child safety (Ofcom, 2025c). Service design, such as group chats, comments sections, and reminders of past interactions, can trap children in harmful content loops and increase their exposure to age-inappropriate, negative materials (Ofcom, 2024a). Platforms are often condemned for promoting harmful content to new and vulnerable users. For example, TikTok's algorithm has been criticised for rapidly showing content referencing self-harm and suicide to young users (RTÉ, 2024).

Online harms affect children unequally. Some children, depending on various mediating factors, circumstances, and individual differences, may face a higher probability of experiencing harm (Ofcom, 2025). Gender differences also appear to play a role, with boys facing a higher risk of encountering violent content compared to girls, while teenage girls aged 13-16 are more likely to experience harassment and abuse (Internet Matters, 2024). Ethnicity can also increase the risk of exposure to online harms, with 4 in 10 girls reporting experiencing sexual harassment online because of their ethnicity (Plan International, 2020).

The nature of online harms varies, from exposure to explicit pornographic material, including audio pornography, to suicide content that encourages self-harm, provides instructions and even romanticising or glorifying such acts (Center for Countering Digital Hate, 2022; Children's Commissioner, 2023; Ofcom, 2022a). Social media platforms, such as TikTok, are reportedly being condemned for feeding young teenagers harmful content such as videos directly referencing self-harm and suicidal thoughts (RTE 2024). Other types of online harms include exposure to abuse and hate content based on characteristics such as gender, sexual orientation or race, linked to misogyny and intersectional harms like 'misogynoir' (Ofcom, 2024b, 2025a; Yonder Consulting, 2022). Harmful behaviours that occur both offline and online environments are also often exacerbated by exposure to bullying and violent content. This includes depictions of violence in games, engagement in risky behaviours such as substance use and misuse, or participation in dangerous stunts and challenges (Family Kids &Youth, 2024; Lérida-Ayala et al., 2023; Moreno-López & Argüello-Gutiérrez, 2025). Children are also increasingly exposed to body stigma content, and depression content that promotes feelings of hopelessness, despair, or depression, all exacerbating mental health issues (Dyer, 2022; Health and Social Care Committee, 2022; Keles et al., 2020; Miller et al., 2025; Office of the Surgeon General, 2023).

Sexual predators are grooming children under six into performing “disturbing” acts of sexual abuse via phones or webcams (Vallance, 2024). The Internet Watch Foundation (IWF) reported that it had discovered more than two thousand remotely filmed child abuse images of three to six-year-olds online in 2023 (Internet Watch Foundation, 2024). Ofcom (2023a,b) also reports that one-third of parents whose children aged 5–7 browse social media allow them to do so unsupervised, exacerbating vulnerability to grooming and exploitation (Vallance, 2024).

The impacts of exposure to child online harms range from poor mental health to physical harms, and cumulative harm (Ofcom, 2025d). Exposure to online harmful content is strongly associated with long-lasting negative impacts on the mental and physical health of young viewers, leading to depression, anxiety, eating disorders, psychiatric illnesses, and even suicidal ideation (Farok & Mahmud, 2020; Hamilton et al., 2021; Padín et al., 2021; Weigle & Shafi, 2024). Young people’s cognitive and emotional development can be severely affected by repeated exposure to inappropriate or harmful material at critical developmental stages. For example, exposure to pornographic materials at an early age can normalise and promote harmful sexual behaviours and attitudes. Online harmful content, such as child sexual images, promoting violence, terrorism, online child grooming or promoting risky behaviours (e.g., eating disorders) can cause long-lasting harm to children and young people (Herbert Smith Freehills, 2025; Hudson et al., 2022; Ofcom, 2022b). Serious emotional harms reported include feelings of shame, anxiety, and distress (especially linked to eating disorders and self-harm content). Broader societal impacts include the normalisation of knife-carrying and harmful attitudes toward women and girls. In the most extreme cases, exposure to harmful content has contributed to loss of life (Ofcom, 2024c, 2025f).

2. Overview of Key Issues

The risks children face online are multifaceted and continuously evolving due to the rapid advancement of digital technologies, including Generative Artificial Intelligence (GenAI), Virtual Reality (VR), gaming platforms, and the commodification of sexual interactions. This section provides an overview of emerging and persistent online harms affecting children and young people.

2.1 Generative AI and algorithmic amplification

2.1.1 Harms created and amplified by GenAI

While harmful content can be self-generated, growing evidence suggests that Generative Artificial Intelligence (GenAI) tools are increasingly used to generate and distribute harmful materials targeting children (Internet Watch Foundation, 2023). Global evidence suggests that GenAI and augmented reality (VR) are emerging technologies linked to increased risks, such as synthetic pornographic content and harmful eating disorder content. AI-powered recommendation engines can also exacerbate harm by rapidly pushing vulnerable young users toward increasingly harmful content streams (e.g., body image disorders, self-harm encouragement). A recent report by the NSPCC suggests that GenAI is increasingly used to perpetuate sexual harassment, bullying, sexual grooming, child sexual exploitation/abuse, and creating harmful ads and recommendations (NSPCC, 2025).

The Europol Innovation Lab Observatory warns that by the end of 2025, 90% of all online content will be AI-generated, including pornographic materials, such as deepfakes (Europol Innovation Lab, 2022). The proliferation of 'nudifying' tools and apps, instructional material and forums that perpetuate content on creating and using 'deepfake' poses increased the risk of harms, particularly among women and girls (Ofcom, 2025g, 2025h). The speed, scale, and anonymity offered by GenAI technologies significantly increase the risks of exposure, exploitation, and the normalisation of harmful behaviours among minors.

Beyond direct harms, UNICEF (2024) warns that generative AI systems are reshaping children's digital environments at an unprecedented pace, embedding persuasive AI agents into social, educational, and entertainment platforms. This raises critical concerns about children's vulnerability to disinformation, the erosion of online trust, privacy intrusions, and the subtle shaping of children's worldviews and behaviours through synthetic agents.

2.1.2 Algorithmic content feeds and exposure to unselected material

Algorithms play a significant role in exposing children to harmful content, including eating disorder and self-harm content. Feed algorithms on platforms such as TikTok, YouTube, and Instagram do not strictly reflect user-initiated choices. Instead, they prioritise:

- Content designed to maximise engagement (e.g., sensationalist, emotionally provocative, extreme).
- Popular or trending material, regardless of user age or vulnerability.
- Rapid, continuous exposure ("infinite scroll" mechanisms).

This system often pushes children towards harmful material they would not have deliberately sought out. For example:

- Young users watching child-friendly videos on YouTube are only a few algorithmic steps away from encountering violent or sexually explicit content (Halliday, 2013; Radesky, 2020)
- TikTok's "For You Page" dynamically surfaces new material based on behavioural signals rather than conscious selection, exposing new users to self-harm, body image, or drug-related content within minutes (RTÉ, 2024).

A recent Ofcom report (2025) suggests that harmful content is becoming normalised and an unavoidable part of many children's online lives.

2.2 Design features and platform functionalities

The design of online platforms plays a crucial role in safeguarding or exposing children to risk. Extant evidence highlights that certain design features and functionalities significantly exacerbate children's exposure to online harms (Ofcom, 2022a, 2022b).

2.2.1 Risk-enhancing features

Several additional design elements further intensify risks for children:

- **Anonymity features:** Allowing users to create accounts without strong verification of identity or age, making it easier for predators to pose as peers.
- **Gamification and reward loops:** Features that encourage persistent engagement and sharing through badges, likes, lootboxes and rewards can pressure young users into risky behaviours such as purchasing digital items to gain social approval and to progress in games.
- **Live streaming:** Platforms enabling live broadcast often lack sufficient real-time moderation, increasing the risk of abuse or coercion during livestream interactions.
- **Infinite scrolling:**
  This design keeps users engaged for extended periods without natural stopping points, which can lead to excessive screen time and exposure to harmful content.
- **Auto-play functions:** Automatically playing the next video or game segment reduces user control and can inadvertently expose children to inappropriate or addictive material.
- **Push notifications:** Frequent alerts can prompt impulsive engagement, distract from offline responsibilities, and reinforce compulsive usage patterns.

2.2.2 Expanding networks beyond known contacts

Many platforms, especially social media and video-sharing apps, use features that encourage users to rapidly expand their networks, often connecting with individuals they have never met offline.

As platforms continue to employ strategies such as automatic friend suggestions based on minimal shared connections (Ofcom, 2022a; Parveen & Varma, 2021), follower recommendations based on algorithmic activity rather than user intention (Narayanan Arvind, 2023; Shehu, 2017), or open direct messaging channels with strangers without prior approval (Substance Abuse and Mental Health Services Administration, 2024), children become potentially the most vulnerable users of these platforms (American Psychological Association, 2024). These functionalities reduce children's control over who they interact with online, increasing the likelihood of exposure to grooming, harassment, or unsolicited harmful content.

2.3 Technology-facilitated commodification of youth sexual interactions

The integration of commercial and social incentives into children's online sexual interactions represents a disturbing development.

Young people today are exposed to environments where personal imagery becomes a transactional commodity, traded for money, gifts, online followers, or social access.

Recent research highlights an alarming trend: the commodification of sexual interactions involving minors in online environments (Thorn, 2021, 2023, 2025). Specifically, the Thorn report (2025) suggests:

- One in three (36%) young people reported being solicited to send sexual imagery by an online-only contact before the age of 18.
- Most solicitations occurred within one week of meeting online.
- One in seven (15%) young people reported engaging in at least one form of transactional sexual experience while underage, exchanging imagery for money, goods (e.g., gaming credits, beauty products), or social opportunities (e.g., followers, party invites).
- Emerging "buyer dynamics" show that 42% of those who engaged in such exchanges believed their buyer was another minor, challenging the traditional assumption that all exploiters are adults.

The commodification of self-generated sexual content (SG-CSAM) blurs the line between voluntary sharing and exploitation, especially when minors view transactions as "consensual" or driven by social pressures rather than explicit coercion. Particularly vulnerable groups include LGBTQ+ youth and younger children (under 13), who report higher rates of such solicitations.

This evolution demands urgent policy recognition. Prevention efforts must address non-monetary incentives (social media influence, online status) as significant exploitative drivers alongside traditional commercial sexual exploitation of children (CSEC).

According to the Thorn report (2025), key dynamics include:

- Fast-trust online cultures (building relationships very quickly online) normalise risky behaviour.
- Non-traditional buyers, including peers, now actively solicit sexual content.
- Social incentives (e.g., gaining followers, popularity) are just as powerful as monetary incentives in driving exploitation.
- Non-explicit commodified requests (e.g., foot photos) are increasingly common, lowering children's perception of risk.

2.4 Gaming platforms

Online gaming platforms, particularly massively multiplayer online games (MMOs) and live-streaming services, are increasingly popular among children and teenagers (Ofcom, 2024; Cabeza-Ramírez et al., 2021). However, these spaces also present distinct risk vectors such as:

- **Grooming within games:** Predators use in-game chat functions, friend systems, and private messaging to establish trust and exploit minors (Internet Watch Foundation, 2024).
- **Microtransactions and gambling risks:** Loot boxes, skin betting (a form of gambling where virtual in-game items are used as currency), and other monetisation strategies introduce children to gambling-like behaviours (Ash et al., 2022).
- **Exposure to Inappropriate content:** Many games expose players to violent, sexualized, or discriminatory content, often without effective moderation (Bègue et al., 2017; Moreno-López & Argüello-Gutiérrez, 2025).
- **Radicalisation risks:** Extremist groups have reportedly used gaming environments to recruit vulnerable young people by exploiting social features (Ofcom, 2024a).

2.5 Virtual reality platforms

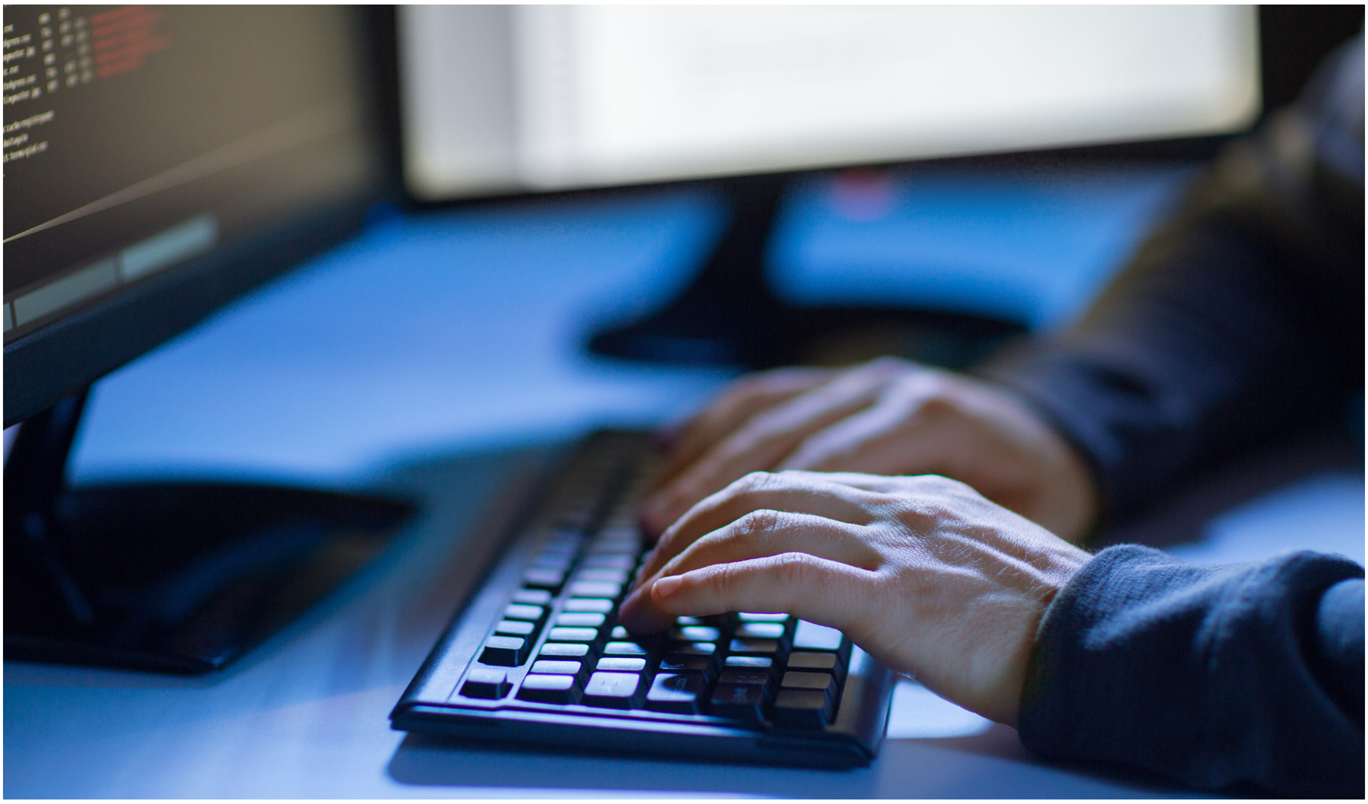
Virtual reality (VR) platforms – often referred to as "metaverses" – are immersive and persistent online environments underpinned by 3D and extended reality (XR) technologies, enabling the blending of physical and digital worlds in real time. Users, including children, typically interact in these virtual spaces through avatars: digital identities that can pose unique challenges compared to real-life identities, as they may extend beyond real-world traits and not necessarily match who users claim to be. A 2022 study conducted in the US found that 26% of teenagers owned a VR device, with 17% using it weekly, and 5% using it daily (Piper, 2022). In the UK, VR access and usage are also increasing. and evidence indicates that children younger than 13 years old are engaging with VR technology, despite their being below established age limits (Limina Immersive & IET, 2022).

The Virtual Reality Risks and Responses for Children (VIRRAC)

The VIRRAC project, led by Prof Davidson and Prof Martellozzo, focused on understanding the risks and harms that children and young people encounter in immersive virtual environments. It explored practical, child-centred solutions that can enhance safety and well-being in the metaverse (Davidson et al., 2025). Research from the VIRRAC project found that many young participants cherish the imaginative, creative and exciting opportunities the metaverse offers (Davidson et al., 2024). Children reported enjoying activities such as exploring new worlds, building entire virtual cities, and experimenting with custom avatars. While metaverses offer exciting new educational and leisure experiences, they also present distinct risks that demand careful consideration. A study by the University of East London and Middlesex University (the VIRRAC project) worked with children and young people from both primary and secondary schools, between the ages of 8 to 18. The VIRRAC project found that young people are already encountering a range of online harms in VR, including harassment, hate speech, or exposure to harmful adult content. Such content can be especially impactful in the metaverse because the high level of immersion makes these experiences feel more intense and "real" than on a flat screen. For instance, incidents of virtual groping or sexual assault in such environments can be traumatic for children, who may feel as though their personal space has been violated. Alarmingly, children as young as nine have reportedly stumbled into 18+ virtual rooms and experienced abuse, highlighting the risk of inappropriate content and contacts when safety-by-design is lacking and controls fail.

- One of the core concerns is online grooming and sexual exploitation in VR. The immersive, avatar-based nature of the metaverse can be exploited by predators who may pose as children or otherwise deceive minors about their identity. Grooming was identified by children as a top perceived risk, with over half of young participants reporting that strangers had approached them asking for personal images or details.

- The children and young people who participated in the VIRRAC project also noted a “lack of avenues for reporting” harmful behaviour on metaverse services. Platforms frequently lack robust age verification, meaning under-13s can access services officially deemed 18+. The anonymity in VR - where anyone can appear as anyone or anything - often encourages offenders and complicates the task of identification, policing and moderation. This anonymity also feeds into identity-related risks like doxing: notably, teenagers in the study feared the malicious revealing of their real identities (“doxing”) almost as much as grooming.
- Children reported either personally experiencing or witnessing hate speech and harassment across metaverse platforms, indicating that real-world biases carry over into virtual identities. Certain groups of children may also be particularly vulnerable in immersive digital environments: those with autism or other special educational needs may find it harder to interpret social cues in VR or to seek help, increasing their susceptibility to bullying or exploitation (Bozgeyikli et al., 2018; Chiappini et al., 2024; Wong KP et al., 2024).
- The psychological and physical impacts of immersive technology on children are still an emerging area of academic research. Experts have warned that intensive VR usage could affect childhood cognitive development and neuroplasticity, given that younger children struggle to distinguish virtual experiences from reality (Drigas & Sideraki, 2024; US PIRG, 2023). Excessive immersion might influence developing brains in unknown ways, and the VIRRAC project’s expert panel raised concerns about possible effects on attention span, impulse control, and even imagination if children spend long hours in virtual worlds. There are also basic physical health considerations: prolonged headset use may cause eye strain or dizziness in children, and there is a risk of injury from moving in physical space without awareness (for example, tripping while “inside” a virtual game). Moreover, the biometric data collected by advanced headsets (such as gaze or heart rate) poses privacy risks if misused, although this is an indirect threat often unnoticed by users.
- In summary, the metaverse offers a novel and enticing opportunity for children but is very much a double-edged sword: on one hand, it can provide rich educational and social benefits; on the other, it exposes users to new and evolving forms of online harm. The “transformative potential” of well-designed VR experiences in supporting learning, creativity, and connection could improve child well-being and online safety, but only if it is underpinned by robust protections and policy solutions.



2.6 Risk of committing cybercrime

Reports of cybercrime have rocketed in the past decade (Payne et al., 2019), and today, the prevalence of cybercrime is believed to transcend traditional crime (Neufeld, 2010). Cybercrime costs the global economy upwards of 10 trillion dollars per year (Fleck, 2024) and this cost is expected to climb annually. With more people online worldwide than ever before, technology has changed the very fabric of modern human life. Increasing evidence suggests that young people, especially, are vulnerable to becoming both victims and perpetrators of cybercrime (Bada & Nurse, 2021; Zhadan, 2023). This article refers to young people as anyone between 15 and 24 years old, in line with the United Nations' definition of youth (United Nations Department of Economic and Social Affairs, 2013). Online perpetrators are a novel phenomenon and do not mirror the profile of what might be considered a traditional criminal (Aiken et al., 2016). Cybercriminals are likely to be younger (Payne et al., 2019) and the characteristics, risk factors and modus operandi of a cybercriminal do not necessarily reflect those of a traditional criminal (Greco & Greco, 2020). Although the motivations of cybercrime are multifaceted and are likely to depend on the type of online crime committed, young cybercriminals appear to be motivated to varying extents by entertainment, peer recognition, financial gain, hacktivism, revenge, or exposure to opportunities to engage in online offences (Leukfeldt & Holt, 2022; Pogrebna & Skilton, 2019; Vaishy & Gupta, 2021). Cybercrime moves fast, and cybercriminals are quick to adapt and evolve. Online safety worldwide depends on a collaborative, cross-sector effort to better understand cybercrime perpetration. Yet, despite the prevalence of online crime and the growing public concern, research and policy are struggling to keep up (Reyns, 2019). This gap in primary research, and evidence-led solutions for policy highlights the critical need for multi-disciplinary approaches that seek to better understand and respond to the cybercrime epidemic.

The CC-DRIVER project

CC-DRIVER (Davidson et al., 2022) (2019-2022) was a large-scale EU project focused on understanding the technical and human factors behind cybercrime, delivered by a consortium of 13 multi-disciplinary partners across Europe. The team at ICC, UEL led the strands of the CC-DRIVER research focusing on the human factor of youth cybercrime, specifically exploring cybercriminal pathways, drivers and motivations. More than 8,000 adolescents from across nine European countries completed the CC-DRIVER survey. The survey captured technology use, attitudes, personality types, socio-demographics, cybercrime perpetration, and social media use (Davidson et al., 2021). The project supported the taxonomy of cybercrime, marking a key advancement in the conceptual classification of online offending behaviours, which enables more targeted research, policy formulation, and intervention strategies tailored to specific offender profiles and motivations (Phillips et al., 2022). The findings revealed that approximately 69% of respondents had participated in some form of online risk-taking or illicit cyber activity.

Several risk factors were identified, including high impulsivity, low parental oversight, weak school engagement, and prior experiences of victimisation such as bullying. Peer influence and involvement in unsupervised online communities also contributed significantly to cyber-offending behaviour. Conversely, protective factors such as strong family support, digital literacy, awareness of legal consequences, and participation in pro-social digital activities were found to reduce the likelihood of offending. Further findings from the project explored the intersection of adolescent online sexual behaviours, such as sexting, sharing explicit images, and viewing pornography, and mental health (Davidson, Aiken, et al., 2024). Adolescents engaging in these behaviours were found to experience higher levels of depression, anxiety, and stress, with those involved in multiple types of risky sexual behaviour reporting the greatest psychological burden. These insights highlight the complex interplay between online behaviours and adolescent well-being, reinforcing the need for holistic interventions that address both behavioural risks and underlying mental health issues.

Young people are increasingly being drawn into committing crime online (Davidson et al, 2022) as well as being the proportionate victims of online crime. While known pathways into youth cybercrime are complex (Davidson, Aiken and Amann, 2016) young people are progressively spending excessive and unrestricted time online, and crossing the moral and legal threshold, often unknowingly. Engaging in harmful or illicit activities in cyberspace can have severe ramifications for young people and their futures. Despite this, the UK's National Crime Agency (NCA) found that children as young as 12 years old are at risk of becoming involved in cybercrime, while one in five children report to have engaged in illicit activities online (NCA, 2025). Considering the complex plethora of online harms that children and young people face, it is vital that younger generations are equipped, safeguarded and empowered to behave appropriately across unmonitored and public online platforms.

3. The UK Government response(s)

The UK Government has introduced several regulatory frameworks to address child online safety. These responses reflect an evolving recognition of the risks presented by digital technologies but vary in their comprehensiveness and effectiveness in tackling emerging threats such as those created by AI, immersive platforms, and commodified sexual interactions.

3.1 The Online Safety Act 2023

The UK Online Safety Act 2023 (UK Government, 2023) represents the UK's flagship legislative effort to regulate online services and protect users from harm.

It sets out the online safety regulations that tech companies that operate a wide range of online services (e.g., user to user services, search services) must follow to keep users, especially children, safe online (eSafety Commissioner, 2024; Ofcom, 2023).

The phased implementation of the Online Safety Act highlights stricter obligations for providers to protect children online. 'Regulated providers' refers to any online service provider falling within the Act's scope (Herbert Smith Freehills, 2024). The Act mandates that companies remove illegal content swiftly and prevent such content from appearing online. This includes content related to terrorism, child sexual abuse, revenge pornography, and more. Additionally, the Act introduces measures to prevent children from accessing harmful or age-inappropriate content like pornography and content promoting self-harm or eating disorders. To ensure compliance, the Act enforces rigorous age verification processes and demands that platforms be transparent about the risks posed to children, with high penalty fines for non-compliant companies.

3.2 Ofcom's Regulatory Role and Children's Access Guidance (2025)

Ofcom has been appointed as the principal regulator for the Online Safety Act.

Key initiatives include:

- **Children's Access Assessments** (2025a), which oversees the implementation of the Act, aims to support age assurance and to ensure that checks are currently done to determine users' age.
- **Highly Effective Age Assurance Standards** (Ofcom, 2025b), which sets expectations for what constitutes effective age verification technologies, including biometric systems, where proportionate. The guidance aims to protect children from hosting, sharing or accessing content that "directs or encourages them to circumvent age assurance process or access controls." (Ofcom, 2025e). This regulation is particularly welcome following evidence that online safety is experienced differently by children across different age groups (The Office of the Children's Commissioner for England, 2022).

3.3 Codes of Practice: Protecting Children Online

In addition to general risk mitigation guidance, Ofcom conducted a series of consultations in preparation for codes of practice to protect children online (Ofcom, 2024d).

In April 2025, Ofcom published the Protection of Children Codes and Guidance (Ofcom, 2025f), a comprehensive set of child protection codes under the Online Safety Act, introducing over 40 mandatory safety measures for online services accessed by UK children. These include requirements for safer content feeds through algorithmic filtering of harmful material, highly effective age assurance systems, rapid content removal procedures, and tools that empower children to manage their online experiences, such as muting, blocking, and disabling comments. Platforms must also provide age-appropriate support resources and ensure that reporting mechanisms are clear and accessible to children. Critically, all services must appoint a senior individual responsible for child safety and conduct annual reviews of risk management. These rules mark a significant regulatory shift, with enforcement powers including fines and service restrictions for non-compliance and signal a new era of accountability in protecting children online. However, there are clear gaps in the legislation, and it is unclear how the OSA will address the challenges raised by new technologies, particularly given the focus upon content and not contact, one of the key risks facing children on VR platforms.

3.4 Cyber Security of AI: Code of Practice (2025)

The Code of Practice for the Cyber Security of AI, published by the UK Government in January 2025, is part of a two-stage intervention to address any type of cybersecurity risks to AI (Department for Science, 2025). This Code of Practice includes neural networks, such as GenAI, and it is part of the UK Government's measures to protect online users, particularly children and young people, from being exposed to online risks and harms, including those generated by AI.

In addition to these efforts, the 5Rights Foundation has published the Children and AI: Code of Conduct (5Rights Foundation, 2025), which sets out a robust framework to ensure that AI systems are developed and deployed in ways that respect and uphold children's rights by design and by default. The Code articulates 12 core principles, such as safety, fairness, transparency, accountability, and the right to be heard and protected, and urges developers, providers, and regulators to embed these standards throughout the AI lifecycle. It specifically highlights the need to address the distinct vulnerabilities of children in digital environments shaped by AI, including the risks of manipulation, profiling, and exposure to inappropriate or harmful content. These risks are amplified by the complexity and opacity of many generative AI systems. The 5Rights framework offers a rights-based complement to technical and regulatory measures, reinforcing the importance of ethically grounded, child-centred AI governance.

3.5 Broader context: international and cross-platform cooperation

In an increasingly interconnected digital world, where children's online lives know no borders, it is essential to act locally, nationally, and internationally to protect children across all settings (Canadian Centre for Child Protection, 2019). In addition to regulatory efforts, considerations must be given to global frameworks focused on children's rights that underpin AI governance, regulatory measures, and protective global efforts to better serve the rights of children.

UNICEF has called for the urgent integration of the principles of the UN Convention on the Rights of the Child, such as non-discrimination, respect for the views of the child, best interests of the child, and the right to life, survival and development, into the design, deployment and regulation of AI technologies. Given the cross-border nature of digital risks, safeguarding children effectively will require not only international cooperation between governments and platforms, but also a rights-based approach that ensures children's well-being, participation and protection are at the centre of all AI and digital innovation efforts (Nylund, 2024).

4. Recommendations and Future Directions

As digital technologies and online environments evolve, safeguarding children and young people requires coordinated, future-facing action. Cross-platform collaboration, data-sharing on emerging harm patterns, and international harmonisation of safety standards will be critical to tackling risks that no single nation or platform can address alone.

4.1 Design levels safeguards

- **Safety-by-design:** Embed safety features from the outset in all digital environments, particularly in VR and immersive platforms. This includes robust age assurance, moderation tools, and accessible safety controls that children can activate during real-time interactions.
- **Privacy-by-design:** Enforce stringent data minimisation and privacy protections, especially regarding children's biometric and behavioural data collected by immersive or AI-enabled technologies.
- **Inclusive and age-appropriate design:** Digital services must consider diverse developmental needs and vulnerabilities, including those of neurodivergent children and children with disabilities. Platforms should default to high privacy and safety settings and adapt content accordingly.

4.2 Regulation and governance

- **Update legislation for emerging tech:** Amend existing safety regulations to explicitly address risks posed by immersive environments, including grooming, harassment, and doxing in VR/metaverse spaces.
- **Accountability in platform architecture:** Shift focus from user responsibility to platform accountability by regulating design elements such as infinite scroll, push notifications, loot boxes, and algorithmic amplification of harmful content.
- **Mandatory risk assessments:** Require companies to conduct transparent and independent risk assessments that consider not just content, but also contact, conduct, and contract risks, particularly in the context of generative AI and recommender systems.

4.3 Systemic reform and collaboration

- **Multi-stakeholder coordination:** Facilitate ongoing cooperation between government, tech industry, academia, law enforcement, educators, and child-safety organisations to develop harmonised safety standards and share data on emerging threats.
- **Child and youth participation:** Embed the voices of children and young people in platform design, policy development, and regulatory review processes. Solutions must reflect children's lived experiences and needs.
- **Ongoing monitoring and evaluation:** Implement mechanisms for continuous review of platform impacts, supported by longitudinal research into the long-term developmental and mental health consequences of digital engagement.

4.4 Research and practice investment

- **Address evidence gaps:** Fund and prioritise longitudinal studies to understand how cumulative exposure to harmful online content affects mental health, cognitive development, and social behaviours.
- **Strengthen preventive interventions:** Equip educators, healthcare professionals, and parents with the tools to identify and mitigate harm early, with particular emphasis on digital literacy, emotional resilience, and pro-social online behaviour.
- **Recognise the risk of offending:** Draw on insights from the CC-DRIVER project to prevent youth cybercrime by addressing contributing factors such as low parental oversight, peer pressure, impulsivity, and exposure to online exploitation.

4.5 Towards a safer digital future

Despite recent legislative progress, most notably, the UK's Online Safety Act (2023) and Ofcom's Code of Practice (Ofcom, 2025e), structural gaps remain in how policy addresses the root causes of harm, namely, platform design and algorithmic practices. Regulatory frameworks must evolve to:

- Move beyond reactive content moderation to enforce pre-emptive design accountability.
- Harmonise international standards for platform responsibility and cross-border enforcement.
- Maintain a balanced approach that protects without over-restricting children's rights to participation, privacy, and access to information.

5. Conclusion

This report has provided a detailed examination of the complex and evolving landscape of online harms facing children and young people, underpinned by emerging technologies such as GenAI, immersive platforms, and exploitative platform design. It underscores the urgent need for a coordinated, evidence-based, and child-centred policy response.

To address these challenges, policymakers must move beyond reactive regulation and implement anticipatory, systemic safeguards that prioritise children's rights by design and default. This includes mandating robust age assurance, safety-by-design standards, transparent algorithmic systems, and independent oversight of high-risk technologies. Stronger regulatory alignment is needed between content, contact, conduct, and contract risks, particularly as new platforms blur these boundaries.

For practice, the report recommends embedding child development expertise, co-design with children, and lived-experience insight into platform governance and moderation. Education and frontline services must be equipped with up-to-date tools, training, and guidance to recognise, respond to, and prevent technology-facilitated harms, especially for the most vulnerable groups.

Above all, this report calls for a rights-based, future-proofed digital governance framework that treats child protection not as a bolt-on requirement, but as a fundamental pillar of responsible innovation.

6. References

5Rights Foundation. (2025). Children & AI Design Code: A protocol for the development and use of AI systems that impact children. 5rightsfoundation.com/children-and-ai-code-of-conduct

Aiken, M., Davidson, J., & Amann, P. (2016). Youth pathways into cybercrime. Paladin Capital Group.

American Psychological Association. (2024). Potential Risks of Content, Features, and Functions: A Closer Look at the Science Behind How Social Media Affects Youth. www.apa.org/topics/social-media-internet/psychological-science-behind-youth-social-media.pdf

Ash, J., Gordon, R., & Mills, S. (2022). Between Gaming and Gambling Children, Young People, and Paid Reward Systems in Digital Games.

Bada, M., & Nurse, J. R. C. (2021). Profiling the Cybercriminal: A Systematic Review of Research. 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2021. doi.org/10.1109/CyberSA52016.2021.9478246

Bègue, L., Sarda, E., Gentile, D. A., Bry, C., & Roché, S. (2017). Video games exposure and sexism in a representative sample of adolescents. Frontiers in Psychology, 8(MAR). doi.org/10.3389/fpsyg.2017.00466

Bozgeyikli, L. L., Bozgeyikli, E., Katkoori, S., Raij, A., & Alqasemi, R. (2018). Effects of virtual reality properties on user experience of individuals with autism. ACM Transactions on Accessible Computing, 11(4). doi.org/10.1145/3267340

Cabeza-Ramírez, L. J., Muñoz-Fernández, G. A., & Santos-Roldán, L. (2021). Video game streaming in young people and teenagers: Uptake, user groups, dangers, and opportunities. Healthcare (Switzerland), 9(2). doi.org/10.3390/healthcare9020192

Canadian Centre for Child Protection. (2019). Protecting Your Child: reduce the risk of child sexual abuse.

Centre for Countering Digital Hate. (2022). Deadly by Design: TikTok pushes harmful content promoting eating disorders and self-harm into young users' feeds. counterhate.com/research/deadly-by-design

Chiappini, M., Dei, C., Micheletti, E., Biffi, E., & Storm, F. A. (2024). High-Functioning Autism and Virtual Reality Applications: A Scoping Review. In Applied Sciences (Switzerland) (Vol. 14, Issue 7). Multidisciplinary Digital Publishing Institute (MDPI). doi.org/10.3390/app14073132

Children's Commissioner. (2023). Evidence on pornography's influence on harmful sexual behaviour among children. www.childrenscommissioner.gov.uk/resource/pornography-and-harmful-sexual-behaviour

Davidson, J., Aiken, M., Gekoski, A., Netuveli, G., Farr, R., & Deac, A. (2024). Understanding Adolescent Criminal and Risky Online Sexual Behaviors in the Context of Mental Health and Well-Being: Findings from a Multi- National European Cybercrime Study. Victims and Offenders. doi.org/10.1080/15564886.2024.2408675

Davidson, J., Aiken, M., Gekoski, A., Phillips, K., & Farr, R. (2021). Research on Protection of Minors: A literature reviews and interconnected frameworks. www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/216479-vsp-harm-guidance/associated-documents/secondary-documents/uel-report-protection-of-minors.pdf

Davidson, J., Aiken, M., Phillips, K., & Farr, R. (2022). European Youth Cybercrime, Online Harm and Online Risk Taking: 2022 Research Report. London, United Kingdom Institute for Connected Communities, University of East London.

Davidson, J., Aiken, M., Phillips, K., & Farr, R . (2021). CC-DRIVER: European Youth Survey. www.ccdriver-h2020.com/_files/ugd/0ef83d_a8b9ac13e0cf4613bc8f150c56302282.pdf

Davidson, J., Martellozzo, E., Farr, R., Bradbury, P., & Meggyesfalvi, B. (2024). VIRRAC Toolkit Report: Virtual Reality Risks Against Children.

Davidson, J., Martellozzo, E., Farr, R., Bradbury, P., & Meggyesfalvi, B. (2025). Virtual Reality Risks Against Children: Roundtables Report. repository.uel.ac.uk/download/1c3f56cb31405a730ea43c7ef0a1dd462ac4d444f844d369223556a8ea822a5a/744429/Final_VIRRAC%202%20Report%202025.pdf

Department for Science, I. & T. (2025). Code of Practice for the Cyber Security of AI. www.gov.uk/government/publications/ai-cyber-security-code-of-practice/code-of-practice-for-the-cyber-security-of-ai

Drigas, A., & Sideraki, A. (2024). Brain Neuroplasticity Leveraging Virtual Reality and Brain–Computer Interface Technologies. In Sensors (Vol. 24, Issue 17). Multidisciplinary Digital Publishing Institute (MDPI). doi.org/10.3390/s24175725

Dyer, C. (2022). Social media content contributed to teenager's death 'in more than a minimal way,' says coroner. BMJ (Clinical Research Ed.), 379. doi.org/10.1136/bmj.o2374

eSafety Commissioner. (2024). Safety by Design puts user safety and rights at the centre of the design and development of online products and services. www.esafety.gov.au/industry/safety-by-design

Europol Innovation Lab. (2022). Facing reality? Law enforcement and the challenge of deepfakes: An Observatory Report from the Europol Innovation Lab. doi.org/10.2813/158794

Family Kids &Youth. (2024). Understanding Pathways to Online Violent Content Among Children. www.ofcom.org.uk/__data/assets/pdf_file/0026/280655/Understanding-Pathways-to-Online-Violent-Content-Among-Children.pdf

Farok, N. H. M., & Mahmud, N. (2020). The influence of social media on suicidal ideation: a systematic literature review. Journal of Research in Psychology, 2(1).

Fleck, A. (2024, April 29). Cybercrime Expected to Skyrocket in Coming Years, Crime Worldwide, Statista. www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027

Foundation, I. W. (2024). Under sixes manipulated into 'disturbing' sexual abuse while playing alone online as IWF says regulation can't wait. www.iwf.org.uk/news-media/news/under-sixes-manipulated-into-disturbing-sexual-abuse-while-playing-alone-online-as-iwf-says-regulation-can-t-wait

Greco, G., & Greco, F. (2020). Investigative Techniques in The Digital Age: Cybercrime and Criminal Profiling. doi.org/10.5281/zenodo.3877668

Halliday, J. (2013). YouTube study shows children 'three clicks away from explicit material'. The Guardian. www.theguardian.com/technology/2013/feb/05/youtube-study-explicit-material

Hamilton, J. L., Biernesser, C., Moreno, M. A., Porta, G., Hamilton, E., Johnson, K., Poling, K. D., Sakolsky, D., Brent, D. A., & Goldstein, T. G. (2021). Social media use and prospective suicidal thoughts and behaviors among adolescents at high risk for suicide. Suicide and Life-Threatening Behavior, 51(6). doi.org/10.1111/sltb.12801

Health and Social Care Committee. (2022). The impact of body image on mental and physical health. www.parliament.uk

Herbert Smith Freehills. (2024). The UK Online Safety Act Who is caught by the OSA? www.herbertsmithfreehills.com/insights/key-topics/who-is-caught-by-the-osa

Herbert Smith Freehills. (2025). What is 'harmful content' and what are the key duties under the Online Safety Act to protect children online? www.herbertsmithfreehills.com/insights/2025-01/what-is-harmful-content-and-what-are-the-key-duties-under-the-osa-to-protect-children-online

Hudson, N., David, M., Haux, T., Kersting, F., Macnaboe, L., Mcdonough, T., Phillips, N., Woolfe, E., & Myers, C.-A. (2022). Content and activity that is harmful to children within scope of the Online Safety Bill A Rapid Evidence Assessment. www.natcen.ac.uk

Internet Matters. (2024). Because children deserve a safe digital world. www.internetmatters.org/wp-content/uploads/2025/01/10-Year-Impact-Report-2014-2024-_-Internet-Matters_latest.pdf

Internet Watch Foundation. (2023). How AI is being abused to create child sexual abuse imagery. www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf

Internet Watch Foundation. (2024). Under sixes manipulated into 'disturbing' sexual abuse while playing alone online as IWF says regulation can't wait. www.iwf.org.uk/news-media/news/under-sixes-manipulated-into-disturbing-sexual-abuse-while-playing-alone-online-as-iwf-says-regulation-can-t-wait

Keles, B., McCrae, N., & Grealish, A. (2020). A systematic review: the influence of social media on depression, anxiety and psychological distress in adolescents. In International Journal of Adolescence and Youth (Vol. 25, Issue 1). doi.org/10.1080/02673843.2019.1590851

Lérida-Ayala, V., Aguilar-Parra, J. M., Collado-Soler, R., Alférez-Pastor, M., Fernández-Campoy, J. M., & Luque-de la Rosa, A. (2023). Internet and Video Games: Causes of Behavioral Disorders in Children and Teenagers. In Children (Vol. 10, Issue 1). doi.org/10.3390/children10010086

Leukfeldt, E. R., & Holt, T. J. (2022). Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. Computers in Human Behavior, 126. doi.org/10.1016/j.chb.2021.106979

Limina Immersive, & IET. (2022). Safeguarding the Metaverse Report. www.theiet.org/media/press-releases/press-releases-2022/press-releases-2022-april-june/19-april-2022-generation-vr

Livingstone, S., Davidson, J., Bryce, J., & Batool, S. (2017). Children's online activities, risks and safety: A literature review by the UKCCIS Evidence Group. In The UK Council for Child Internet Safety. www.gov.uk/government/publications/childrens-online-activities-risks-and-safety-a-literature-review-by-the-ukccis-evidence-group

Miller, C., Bubrick, J., & Hamlet, A. (2025). Does Social Media Use Cause Depression. childmind.org/article/is-social-media-use-causing-depression

Moreno-López, R., & Argüello-Gutiérrez, C. (2025). Violence, Hate Speech, and Discrimination in Video Games: A Systematic Review. Social Inclusion, 13. doi.org/10.17645/si.9401

Nagata, J. M., Memon, Z., Talebloo, J., Li, K., Low, P., Shao, I. Y., Ganson, K. T., Testa, A., He, J., Brindis, C. D., & Baker, F. C. (2025). Prevalence and Patterns of Social Media Use in Early Adolescents. Academic Pediatrics, 25(4). doi.org/10.1016/j.acap.2025.102784

Narayanan Arvind. (2023, March 9). Understanding Social Media Recommendation Algorithms. Knight First Amendment Institute at Columbia University. knightcolumbia.org/content/understanding-social-media-recommendation-algorithms

NCA, (2025) Young People & Cyber Criminality, Cyber Choices, www.getsafeonline.org/personal/articles/young-people-cyber-criminality

Neufeld, D. J. (2010). Understanding Cybercrime. Hawaii International Conference on System Sciences. doi.org/10.1109/HICSS.2010.417

NSPCC. (2024). Online harms: protecting children and young people. learning.nspcc.org.uk/news/2024/january/online-harms-protecting-children-and-young-people

NSPCC. (2025). Viewing Generative AI and children's safety in the round. learning.nspcc.org.uk/research-resources/2025/generative-ai-childrens-safety

Nylund, B. V. (2024). How can generative AI better serve children's rights? Looking to the Convention on the Rights of the Child. UNICEF. www.unicef.org/innocenti/how-can-generative-ai-better-serve-childrens-rights

Ofcom. (2022a). Research into risk factors that may lead children to harm online. www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/keeping-children-safe-online/risk-factors-that-may-put-children-at-harm-online/children-risk-factors-report.pdf?v=328565

Ofcom. (2022b). Research into risk factors that may lead children to harm online. www.revealingreality.co.uk

Ofcom (2023a). Children and Parents: Media Use and Attitudes. www.ofcom.org.uk/media-use-and-attitudes/media-habits-children/children-and-parents-media-use-and-attitudes-report-2023

Ofcom. (2023b). Ofcom's approach to implementing the Online Safety Act. www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/roadmap/ofcoms-approach-to-implementing-the-online-safety-act?v=330308

Ofcom. (2024a). A third of children have false social media age of 18+. www.ofcom.org.uk/online-safety/protecting-children/a-third-of-children-have-false-social-media-age-of-18

Ofcom, (2024b). Children and Parents: Media Use and Attitudes Report. www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/children-media-use-and-attitudes-2024/childrens-media-literacy-report-2024.pdf?v=368229

Ofcom. (2024c). Protecting children from harms online. Volume 3: The causes and impacts of online harms to children. www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/284469-consultation-protecting-children-from-harms-online/associated-documents/vol3-causes-impacts-of-harms-to-children.pdf?v=336052

Ofcom. (2024d). Important dates for Online Safety compliance. www.ofcom.org.uk/online-safety/illegal-and-harmful-content/important-dates-for-online-safety-compliance

Ofcom. (2025a). A Safer Life Online for Women and Girls: Practical Guidance for Tech Companies Contents Section. www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/consultation-on-draft-guidance-a-safer-life-online-for-women-and-girls/main-docs/annex-a-draft-guidance.pdf

Ofcom. (2025b). Children's Access Assessments Guidance. www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/childrens-access-assessments-guidance.pdf?v=388843

Ofcom. (2025c). Children's Register of Risks Contents. www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-protecting-children-from-harms-online/main-document/childrens-register-of-risks.pdf?v=396667

Ofcom. (2025d). Guidance on highly effective age assurance and other Part 5 duties.

Ofcom. (2025e). Protecting children from harms online: Codes at a glance. www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-protecting-children-from-harms-online/main-document/codes-at-a-glance.pdf?v=395791

Ofcom. (2025f). The causes and impacts of online harms to children (Vol 2). www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-protecting-children-from-harms-online/main-document/volume-2-the-causes-and-impacts-of-online-harms-to-children.pdf?v=395485

Ofcom. (2025g). Ofcom calls on tech firms to make online world safer for women and girls. www.ofcom.org.uk/online-safety/illegal-and-harmful-content/ofcom-calls-on-tech-firms-to-make-online-world-safer-for-women-and-girls

Ofcom. (2025h). Experiences of using online services. www.ofcom.org.uk/media-use-and-attitudes/online-habits/internet-users-experience-of-harm-online

Office of the Surgeon General. (2023). What Drives Mental Health and Well-Being Concerns: A Snapshot of the Scientific Evidence. US Department of Health and Human Services.

Office of the United Nations High Commissioner for Human Rights (OHCHR). (1989). Convention on the Rights of the Child. www.ohchr.org/sites/default/files/crc.pdf

Padín, P. F., González-Rodríguez, R., Verde-Diego, C., & Vázquez-Pérez, R. (2021). Social media and eating disorder psychopathology: A systematic review. In Cyberpsychology (Vol. 15, Issue 3). doi.org/10.5817/CP2021-3-6

Parveen, R., & Varma, N. S. (2021). Friend's recommendation on social media using different algorithms of machine learning. Global Transitions Proceedings, 2(2). doi.org/10.1016/j.gltp.2021.08.012

Payne, B., May, D. C., & Hadzhidimova, L. (2019). America's most wanted criminals: comparing cybercriminals and traditional criminals. Criminal Justice Studies, 32(1). doi.org/10.1080/1478601X.2018.1532420

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences, 2(2). doi.org/10.3390/forensicsci2020028

Piper, S. (2022). 43rd Semi-Annual Generation Z Survey of 7,100 U.S. Teens. www.businesswire.com/news/home/20220406005379/en

Plan International. (2020). State of the World's Girls 2020: Free to Be Online? plan-international.org/publications/free-to-be-online

Pogrebna, G., & Skilton, M. (2019). A Sneak Peek into the Motivation of a Cybercriminal. In Navigating New Cyber Risks (pp. 31–54). Springer International Publishing. doi.org/10.1007/978-3-030-13527-0_3

Radesky, J. S. , S. A. , Y. S. L. , W. H. M. , & R. M. B. (2020). Young Kids and YouTube: How Ads, Toys, and Games Dominate Viewing.

Reyns, B. W. (2019). Online Pursuit in the Twilight Zone: Cyberstalking Perpetration by College Students. Victims and Offenders, 14(2). doi.org/10.1080/15564886.2018.1557092

RTÉ. (2024). RTÉ Prime Time experiment reveals disturbing content recommended to 13-year-old TikTok users in Ireland. Raidió Teilifís Éireann, Ireland's National Public Service Media. about.rte.ie/2024/04/18/rte-prime-time-experiment-reveals-disturbing-content-recommended-to-13-year-old-tiktok-users-in-ireland/#:~:text=In%20response%20to%20growing%20concerns,an%20age%20of%2013%20years

Shehu, S. (2017). Friend Suggestion System for the Social Network Based on User Behavior. International Journal of Computer Science, Engineering and Information Technology, 7(5). doi.org/10.5121/ijcseit.2017.7502

Substance Abuse and Mental Health Services Administration. (2024). Online Health and Safety for Children and Youth: Best Practices for Families and Guidance for Industry.

The Office of the Children's Commissioner for England. (2022). Digital children: a survey of children and parents. www.childrenscommissioner.gov.uk/resource/digital-childhoods-a-survey-of-children-and-parents

Thorn. (2021). Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking in 2021. info.thorn.org/hubfs/Research/Thorn_ROT_Monitoring_2021.pdf

Thorn. (2023, February 7). New Research from Thorn: 22% of minors report having online sexual interactions with adults. www.thorn.org/blog/new-research-from-thorn-22-of-minors-report-having-online-sexual-interactions-with-adults

Thorn. (2025). Commodified Sexual Interactions Involving Minors: New data on evolving dynamics in technology-facilitated child sexual exploitation. info.thorn.org/hubfs/Research/Thorn_CommodifiedSexualInteractionsInvolvingMinors_Apr2025.pdf

UK Government. (2023). Online Safety Act 2023. www.legislation.gov.uk/ukpga/2023/50/enacted

UNICEF. (2024). Generative AI: Risks and opportunities for children. www.unicef.org/innocenti/generative-ai-risks-and-opportunities-children

United Nations Department of Economic and Social Affairs. (2013). Definition of Youth. undesadspd.org/Youth.aspxfacebook.com

US PIRG. (2023). VR risks for kids and teens. pirg.org/edfund/resources/vr-risks-for-kids

Vaishy, S., & Gupta, H. (2021). Cybercriminals' Motivations for Targeting Government Organizations. 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), ICRITO 2021. doi.org/10.1109/ICRITO51393.2021.9596104

Vallance, C. (2024, April 23). Three-year-olds groomed online, charity warns. BBC. www.bbc.co.uk/news/articles/cx9wezr1d1vo

Weigle, P. E., & Shafi, R. M. A. (2024). Social Media and Youth Mental Health. In Current Psychiatry Reports (Vol. 26, Issue 1). doi.org/10.1007/s11920-023-01478-w

Wong KP, Zhang B, Lai CYY, Xie YJ, Li Y, Li C, & Qin J. (2024). Empowering Social Growth Through Virtual Reality–Based Intervention for Children with Attention-Deficit/Hyperactivity Disorder: 3-Arm Randomized Controlled Trial. JMIR Serious Games, 12. doi.org/10.2196/58963

Yonder Consulting. (2022). Children's Online User Ages Quantitative Research Study. www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/keeping-children-safe-online/childrens-online-user-ages/children-user-ages-chart-pack.pdf?v=328540

Zhadan, A. (2023). Teen cyber cartels: when world's most prolific cybercriminals are minors. Cybernews. cybernews.com/editorial/teen-cyber-cartels

CHILD ONLINE HARMS POLICY
THINK TANK

ICC
THE INSTITUTE FOR CONNECTED COMMUNITIES

University of
East London

Pioneering Futures since 1898

Digital Threats Can’t Wait.
Neither Can We.
Every Child, Every Click, Protected

Contact:

Email: **child.ohptt@uel.ac.uk**

www.uel.ac.uk/child-online-harms-policy-think-tank