Protecting childhood online: Why the Online Safety Act matters

December 2025

Briefing from the Children's Coalition for Online Safety

Introduction

This briefing has been prepared on behalf of the Children's Coalition for Online Safety, a collection of organisations that have worked closely together throughout the development of the Online Safety Act. Through our work with Ofcom and the Government, we have consistently pressed for a regulatory framework that truly delivers for children. We believe that the Act provides an essential foundation for creating a safer digital world – one that protects the future of childhood and upholds children's rights.

Within this briefing, we present the collective evidence gathered by our organisations, demonstrating both the scale and severity of the harms children face online, and how this first-of-its-kind legislation will help to mitigate them. Whilst the Act will not fix these issues in full – and further action is needed to address harm at its source, particularly risky and harmful design practices – it represents a vital first step. We therefore urge MPs to speak in support of the Act's implementation and to champion the continued progress needed to keep children safe online.

Preventing harms to children online

The Online Safety Act delivers unprecedented protection for children online. Tech companies, including social media platforms and search engines, now have a duty of care to prevent children from accessing the most harmful content or being contacted by adults they do not know on their platforms.

Below we note just some of the protections that are now in force for children across the country, and how these measures are already making a difference.

1. Requiring services to prevent exposure to the most harmful content for children, including pornography.

The scale of harm caused by children's exposure to pornography is staggering.

Research by the Children's Commissioner for England found that, by age 11, 27% of children have seen pornography, with the average age of first exposure to pornography being just 13 years old.[1] X (formerly Twitter) is the most common platform where children see pornography (41%), followed by dedicated pornography sites (37%), Instagram (33%), Snapchat (32%) and search engines (30%).[2]

This early exposure to pornography drives harmful attitudes. Research by the Children's Commissioner found 79% of 18-21-year-olds have seen content involving sexual violence before turning 18, and young people aged 16-21-years-old are more likely to assume that girls expect or enjoy physical aggression during sex.[3]

The Act now requires services to prevent children from accessing such content.

The UK's age assurance duties are world-leading, creating essential friction that helps prevent children from accidentally encountering pornography and other harmful content online. Despite reporting of a surge in VPN usage, recent research shows that the spike this summer was not driven by children attempting to circumvent these new protections.[4]

Since the Act has come into force, Pornhub, the most visited pornography site in the world, noted a 77% reduction in visitors to its website since implementing age check measures,[5] a clear illustration of how the Act is working in practice. Further, Ofcom has already

---

[1] Children's Commissioner for England (2023) *'A lot of it is actually just abuse': Young people and pornography*

[2] Children's Commissioner for England (2023) *Growing up with pornography: Advice for parents and schools*

[3] Children's Commissioner for England (2023) *'A lot of it is actually just abuse': Young people and pornography*

[4] Childnet (2025) *Young people's use of VPNs*. See also: Internet Matters (2025) *New data shows no rise in children's VPN use after the introduction of online age checks*

[5] BBC News (2025) *Pornhub says UK visitors down 77% since age checks came in*

launched investigations into 76 pornography providers since provisions came into effect earlier this year.[6]

2. Mandating services prevent predatory contact through default safety measures.

In 2023 alone, 31% of children aged 9-16 surveyed by Internet Matters reported that strangers had tried to contact them online.[7] 5Rights' own research using child-aged avatars revealed that children's profiles can often be sent large volumes of unsolicited messages and requests from unknown users, including adults.[8]

Most recent data from the NSPCC notes that online grooming offences have hit record high levels across the UK, with 7,263 offences recorded in 2024 – double the number from 2017-18.[9] In 2024, the IWF confirmed 291,273 reports of child sexual abuse material. 91% of the reports assessed as criminal were found to contain 'self-generated' imagery.[10]

The Act requires services to take steps to address these escalating harms.

The Act mandates that high-risk platforms turn off location sharing by default for children, prevent children's accounts from being recommended to unknown adults in connection lists and block strangers from contacting children via direct messages.

In response, the Act is driving tech companies to make design changes to comply with its requirements to make safer experiences for children. This includes increased safety measures on popular services used by children, including Meta's Teen Accounts[11] and Roblox.[12]

3. Protecting children from pro-suicide, pro-self-harm and pro-eating disorder content appearing in their feeds.

Research using child avatar accounts from the Centre for Countering Digital Hate (CCDH) found that children on TikTok were shown harmful content every 39 seconds, with content referencing suicide appearing within 2.6 minutes of creating the account and eating disorder content within 8 minutes.[13]

---

[6] Ofcom (2025) *Ofcom fines nudification site £50,000 for failing to introduce age checks*
[7] Internet Matters (2024) *Children's Wellbeing in a Digital World*
[8] 5Rights Foundation (2021) *Pathways: How digital design puts children at risk*
[9] NSPCC (2025) *Data shows how criminals are using private messaging platforms to manipulate and groom children*
[10] Internet Watch Foundation (2025) *IWF Annual Data & Insights Report 2024*
[11] Meta (2025) *Expanding Teen Account Protections and Child Safety Features*
[12] Roblox (2025) *Roblox Requires Age Checks for Communication, Ushering in New Safety Standard*
[13] Centre for Countering Digital Hate (2022) *Deadly by Design*

Despite this, as research from the Molly Rose Foundation shows, only two out of six major social media companies are actively removing potentially self-harm and suicide material.[14]

The Act ensures all services in scope must filter out harmful content from children's feeds.

Reporting by Sky News,[15] which interviewed teenagers before and after the measures came into force, noted that five out of six of the teenagers noticed that their feeds seemed "tamed" compared to before. This includes:

- **16-year-old Liam**, who noted that, regarding eating disorder content, he "used to see them every few scrolls", but since the Act came into force he did not see any; and
- **15-year-old Ryan**, who said his TikTok feed has become "free from violence" since the measures came into force.

Requiring age assurance methods be privacy-preserving

Services hosting high-risk content to children are required to use age assurance technology to prevent children from accessing it. The Act requires that age assurance meets strict standards.[16]

This includes that it must be accessible, proportionate to risk and privacy-preserving, being fully compliant with UK GDPR and the Age Appropriate Design Code.[17]

This includes complying with data protection obligations, such as:[18]

- **Storage limitation**: Data must be deleted once its use has been completed. In the case of age verification to access a porn website, this would mean deleting data once it has been confirmed that the user is over 18.
- **Data minimisation**: Companies can only collect and process the information needed to confirm someone is over 18. Age assurance providers do not need to know someone's full identity. Information collected about users should not allow for excessive data gathering, in line with UK GDPR.
- **Security and confidentiality**: Companies must have security measures in place to protect user data.

We welcome that Ofcom has opened investigations into services not complying with the age assurance duties. However, we would also like to see joint working between both

[14] Molly Rose Foundation (2025) *How effectively do social networks moderate suicide and self-harm content?*
[15] Sky News (2025) *'Tamed' algorithms and plummeting pornography views: Impact of new online safety rules revealed one month on*
[16] Online Safety Act, Schedule 4, 12
[17] Information Commissioner's Office (2021) *Age appropriate design: A code of practice for online services*
[18] Information Commissioner's Office (2024) *Expectations for age assurance and data protection compliance*

Ofcom and the Information Commissioner's Office to ensure that age assurance systems are accountable for their data practices, ensuring they are privacy-preserving.

Ensuring bereaved families get answers when children have died due to online harms, pushing tech companies to fully support coroners with their investigations.

For too long, tech companies have stonewalled bereaved families and coroners investigating children's deaths linked to online harms.

The Act gives Ofcom the power to request information from tech companies on behalf of coroners where there is reason to believe the service may hold information relating to a child's death. This includes information such as content the child viewed or engaged with, how they encountered it and how algorithms and other functionalities may have contributed.

Tech companies will need to provide bereaved families with a helpline, or clear processes for obtaining information in circumstances where a child has died. Tech companies have a duty to respond to these requests in a timely manner and offer a proper complaints process.

These protections were fought for, and continue to be fought for, by the Bereaved Families for Online Safety,[19] including the parents of Molly Russell, Frankie Thomas, Olly Stephens, Archie Battersbee, Breck Bednar, Isaac Kenevan, Jools Sweeney, Maia Walsh, Sophie Parkinson, Brianna Ghey, Murray Dowey, Mia Janin, Christopher Nicolaou, Aimee Walton, Josh Hendy and Lucas Webb.

What is at stake: Children's right to be safe online

Without the protections set out by the Online Safety Act:

- More children encounter harmful content, including pornography, which shapes harmful attitudes about consent and violence;
- More children receive unsolicited contact from unknown adults;
- More children access content that encourages self-harm, eating disorders and suicide; and
- More families are stonewalled by tech companies when seeking answers about their child's death.

Together, with children, families and civil society Parliament has passed legislation that protects children's right to be safe online, prevents the most harmful content from

[19] See: Bereaved Families for Online Safety (2025)

appearing on their feeds, and provides accountability when companies fail to meet their duties of care. Without it, childhood remains at risk.

What more there is to do: Further ways the Online Safety Act can protect childhood in the digital age

The Online Safety Act is an important first step, but there is still much more to do to ensure that childhood is preserved in a digital world. Throughout the implementation of the Act, our organisations have jointly supported proposals that would strengthen the online safety regime to keep children safe.

In order to bring about the changes for children promised by the Act, Government and the regulator must go further. This includes:

- **Requiring services to implement safety by design measures**: Ofcom's codes of practice do not require services to address holistic risks to children's safety on their services, focusing on narrow systems and processes rather than preventing harm upstream. Whilst Ofcom has introduced new measures on proactive technologies in its most recent consultation, these will likely not be implemented for another year, whilst failing to address how digital design leads to harm.
- **Ensuring services uphold their own minimum age limits and age-appropriate design**: It is vital that providers uphold their minimum age requirements to protect the youngest children online. The regulation must be amended to ensure that services are explicitly required to enforce their age limits and deploy age-appropriate design: ensuring the experiences of a 13-year-old and 17-year-old respect their capacities and meet their needs.
- **Addressing addictive design as a harm under the Act**: Children lack the same self-regulation as adults owing to their developing cognition.[20] Yet, the tech company business model – designed to extend use, time engagement spent online – means children are unable to use these products whilst maintaining their agency. The Government must look towards addressing how addictive design practices (e.g. features like dark patterns) can be regulated under the Act.

This briefing is supported by:

5Rights Foundation, NSPCC, Center for Countering Digital Hate (CCDH), Ditch the Label, Online Safety Act Network, Internet Watch Foundation (IWF), Childnet, Children's Media Foundation, Clean Up The Internet, UK Safer Internet Centre, SWGfL, WAVE Trust, Marie Collins Foundation, Lucy Faithfull Foundation and Internet Matters.

[20] See: 5Rights Foundation (2023) *Digital Childhood: Addressing childhood development milestones in the digital environment*