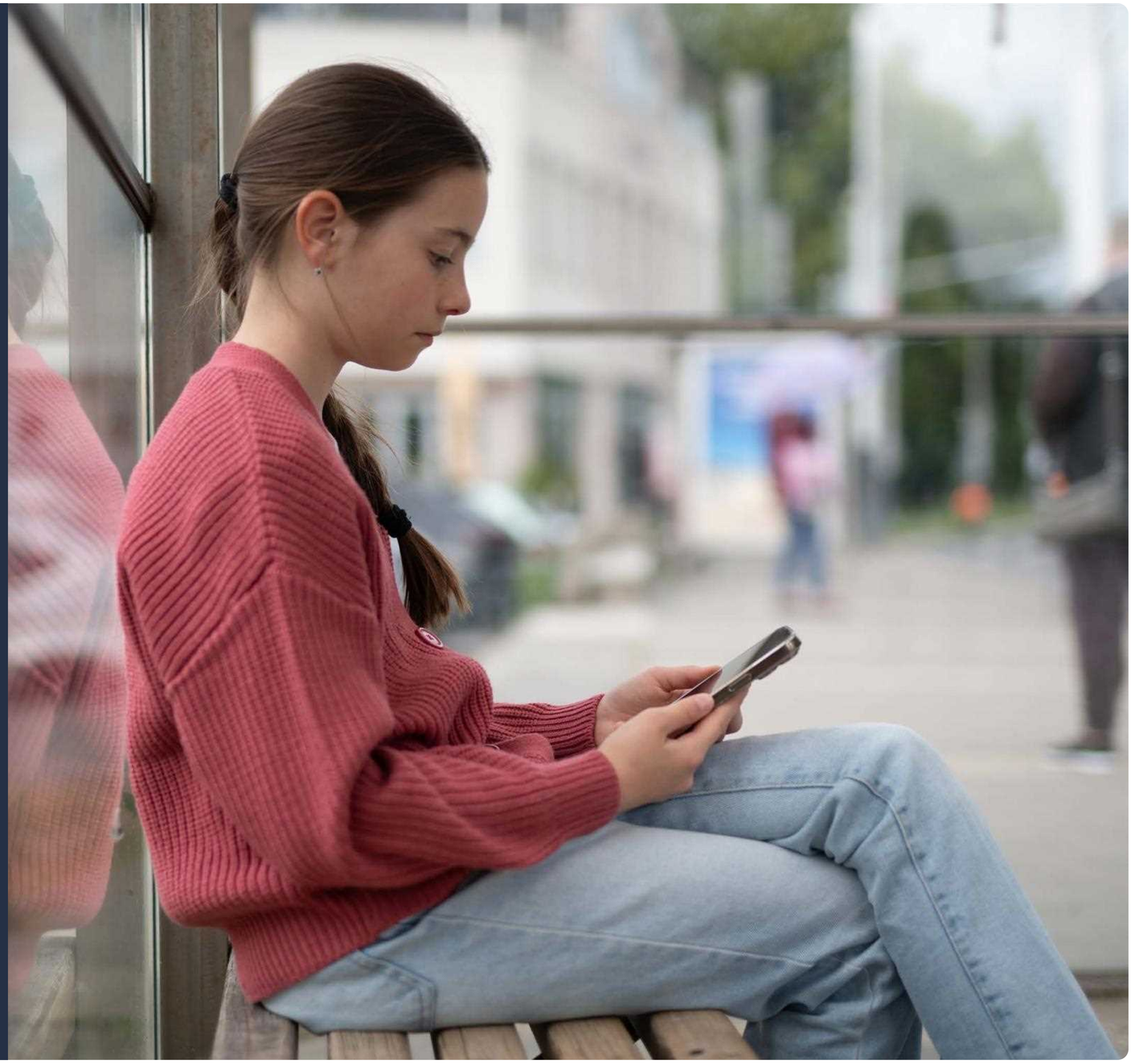
The Online Safety Act: Are children safer online?

May 2026

internet matters.org

Developed with:

BMG an RSK company



Foreword

For most young people, the online world is no longer a distinct space but an integral part of everyday life, with devices providing access to a wide variety of digital platforms from an early age. While this constant connectivity offers significant benefits for entertainment, learning and connection, it also increases children's exposure to potential harms, which has become an ongoing challenge for delivering both effective regulation and support for families.

In the UK, the Online Safety Act has introduced a range of measures aimed at improving online safety for young users; however, questions remain about whether current regulations are sufficiently robust, effectively enforced, and adaptable to an evolving digital landscape. This report explores the impact of the Online Safety Act through the experiences of families. Drawing on survey and focus group data collected soon after the Act's children's safety protections came into force, it provides an early view of how the online landscape is changing, and crucially, where it is not.

Positively, there are clear signs of progress with efforts to improve safety being noticed and supported by both parents and children, such as better reporting tools, more content labelling, and restrictions on certain platform functions. As a result, some families are cautiously optimistic that the online world is becoming safer.

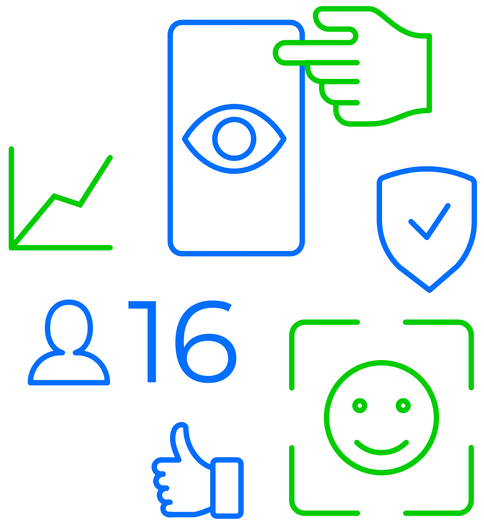
However, children continue to encounter harmful content at concerning rates, and age checks to manage their experiences online - while widespread - are often seen as easy to circumvent. In addition, there are real fears about the rapid growth of AI-generated content and families want more action to help children regulate the time they spend online, a fundamental issue that both parents and children themselves are finding it increasingly difficult to control.

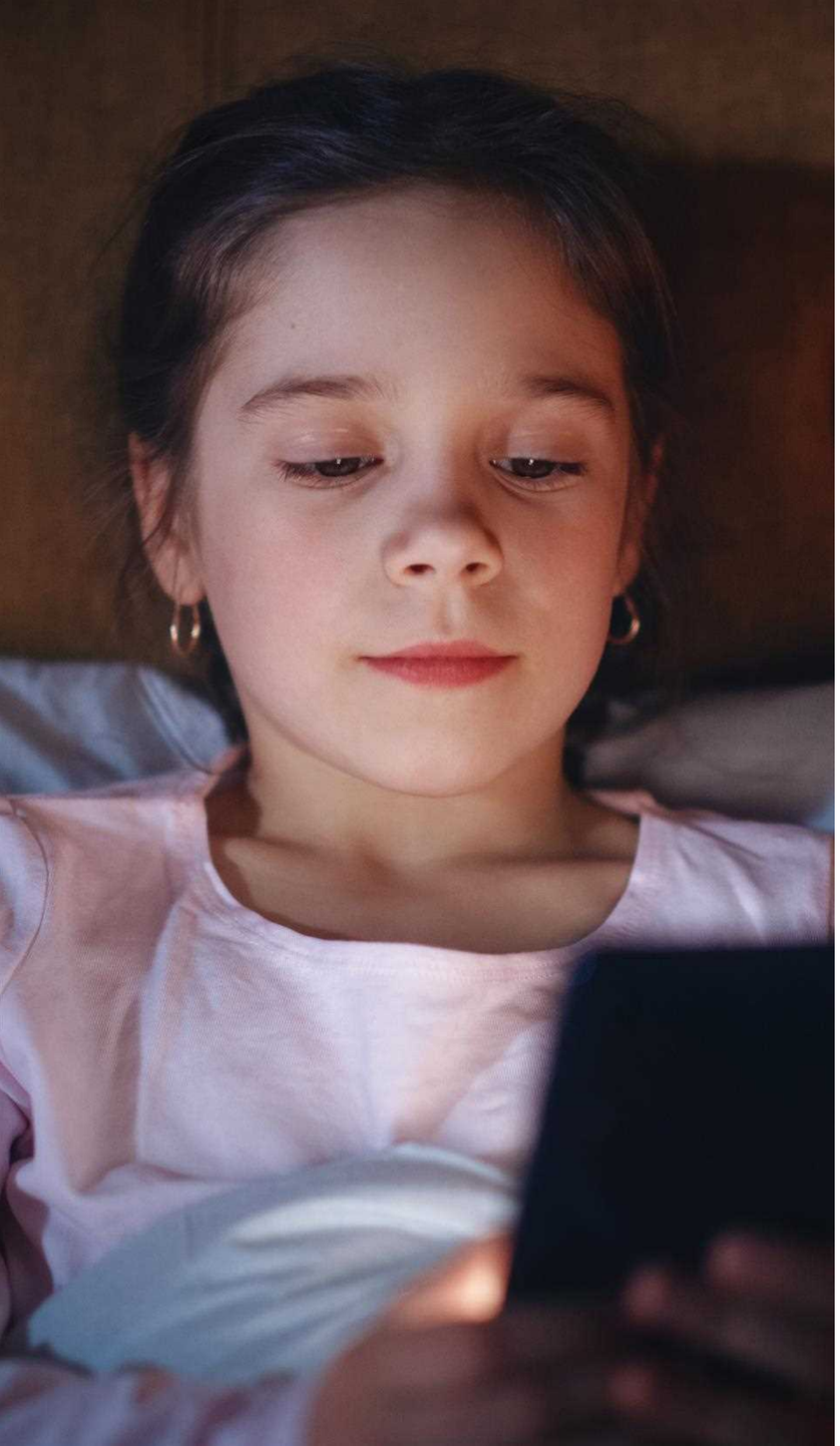
Within this context, parents continue to shoulder much of the responsibility for keeping children safe in an increasingly complex digital environment. While families recognise their role, they are clear that they cannot do this alone. Stronger action is needed from both government and industry to ensure that children can only access online services appropriate for their age and stage and where safety is built in from the outset, rather than added in response to harm.

The UK Government is currently consulting on what more can be done to keep children safe in a digital world, offering a timely opportunity for positive change. Although views may differ on what action is needed, the goal is clear: to support children to thrive online while delivering meaningful protection from harm.

Rachel Huggins
CEO of Internet Matters

Contents





Executive Summary

The past year has been a significant period of change for children's online safety in the UK. New rules under the Online Safety Act (OSA) have come into force, aimed at creating safer online spaces.[1] For many families, however, the pace of change has not been quick enough. As countries around the world take bolder steps – including banning children from social media – pressure is growing on both governments and platforms to go further. Against this backdrop, this report explores what – if anything – has changed in the online lives of families in the UK, since the Act came into force.

Data from surveys and focus groups, collected after the new rules came into effect, shows that some progress is being made. Families are seeing more visible safety measures, and some feel the online world is becoming safer for children. However, the OSA has not delivered the step change needed to meaningfully improve children's online safety and wellbeing. Children continue to encounter harmful content at unacceptable rates, while age verification is widely seen as easy to bypass. Furthermore, many of the issues most important to families, such as managing the amount of time children spend online and the risks of AI, remain unaddressed. As a result, families continue to shoulder the responsibility of keeping children safe online.

By examining the impact of new safety measures from the perspective of children and parents, we can identify where they are falling short and what gaps remain.[2] Using these insights, the report highlights what further action is needed to ensure children can thrive in an online world.

1. *Throughout the report we refer to the Online Safety Act as the OSA or the Act.*
2. *In this report we use the term parent to refer to both parents and caregivers of children. We know that parents and carers go by many names.*

Early evidence of progress

New laws are making safety measures more prominent across children's online spaces, with parents and children largely welcoming these changes.

- **Safety features are increasingly visible.** Around seven in ten children (68%) and parents (67%) report seeing more safety measures including improved reporting tools and content filters, alongside blocks on certain functions such as live streaming or chat. Parents are also seeing changes to parental controls, with 64% of parents noticing new or improved parental controls.
- **Age checks are common and seen as easy to complete.** About half of children (53%) say they have recently been asked to verify their age, most often when setting up new accounts. According to children, the following methods were described as easy: uploading a government ID document (88%), facial age estimation (89%) and using a third-party app (88%).
- **Children are supportive of changes.** Where children have noticed new safety features or changes to functionalities, their views are broadly positive, particularly towards improved blocking and reporting processes (90%). They also view safety measures such as restrictions on contacting certain people (77%) and limits on access to functions like livestreams or comments (74%) as a good thing.
- **Parents and children are optimistic the online world is getting safer for children.** 39% of parents and 42% of children feel it has become safer recently; however, this view is not universal, with 28% of parents and 16% of children believing it has become less safe.
- **Children are seeing more age-appropriate content online.** The majority (54%) of children report that content they have seen online recently is more child friendly.

Where the OSA and its implementation falls short

The legislation is not yet delivering the outcomes needed to measurably improve families' online lives and more can be done to address the key concerns of children and parents.

- **Awareness of how to bypass age checks is widespread.** 46% of children believe age checks are easy to bypass, with only 17% saying they are difficult. Methods discussed include using a fake birthday, a Virtual Private Network or submitting a video of another person's face, or even a character, to trick platforms into estimating an older age.
- **A third of children (32%) say they have bypassed age checks,** including by entering a fake birthdate (13%) or using someone else's login (9%), while others used more creative methods like drawing on facial hair.
- **Some parents help their children bypass checks.** A quarter (26%) of parents have allowed their child to bypass age checks, with 17% actively helping their children and 9% allowing it or "turning a blind eye". Parents say they do this only when they believe the activity is safe.
- **Children continue to encounter harmful content online.** 49% of children said they had experienced harm online recently, including seeing violent content (12%), content that promotes unrealistic body types (11%) and hateful content (including racial or homophobic content) (10%) – all of which should be prohibited under the OSA's Protection of Children Codes. An example discussed in focus groups was the unintentional exposure through social media feeds to the assassination of Charlie Kirk.
- **Managing time online and the risks of AI-generated content are key concerns.** Changes introduced under the OSA are broadly welcomed, but do not address what children and parents describe as their most immediate, day-to-day concern: the amount of time children spend online. Alongside this, children frequently encounter AI-generated videos and images, some of which are difficult to identify as artificial, raising concerns about misinformation and inappropriate content.

What do parents and children want

Families agree that stronger action to keep children safe online is needed, but there are differing views on how this should be achieved.

- **Parents and children want more action to keep children safe online.** Only 22% of parents and 31% of children believe the Government is doing enough to protect children online.
- **Support for a blanket ban on social media is mixed.** Previous Internet Matters research finds 62% of parents support a ban on social media for under-16s.[i] Those in favour argue it will improve children's wellbeing. However, many are concerned that a ban would be ineffective in practice, with this view also being held by some who support a ban. Others think it could be detrimental, given the social and developmental role online spaces play in a digital world. Children too worry that such bans could remove important social connections and support systems.
- **Stronger enforcement of the OSA, stricter age-checks and restricting harmful features were the most popular alternatives to a ban.** Parents support greater involvement in verifying children's ages, and both parents and children support limiting features that encourage prolonged engagement, such as streaks, or increase risk, such as location sharing.

Families can't solve this alone

Parents and children alike recognise that children's online safety is a shared responsibility. While parents ultimately see themselves as responsible, they think more can be done by government and platforms.

Across all online services used by children – including social media platforms, gaming environments and AI chatbots – initiatives to improve children's safety and wellbeing must be based on the following principles:

- **Safety-by-design:** Safety should be built into online services from the start rather than added after harms emerge. It should also be considered before new features or functionalities are added to a platform.
- **Risk-based approach:** Children's access to online services should be determined by the level of risk posed by its features, functionalities and content, and the effectiveness of the safeguards it has in place.
- **Age-appropriate experiences:** Children's access to content and features should be tailored to their stage of development, rather than a one-size-fits-all approach for all children.
- **Highly effective age assurance:** Robust age assurance systems are needed to accurately determine users' ages and implement appropriate protections.
- **Media literacy** equips both children and parents with the skills, knowledge and tools to navigate the online world safely and critically. This should be inbuilt to platforms and supported by schools and government.

Taken together, these principles provide a comprehensive framework for children's online safety.

Methodology

This report is part of Internet Matters' Digital Wellbeing Index research programme.[ii] Each year, Internet Matters surveys 1,000 children and their parents across the UK, providing wide-ranging insights into children's online lives. The research, starting in 2021, tracks trends in children's digital wellbeing and provides a holistic picture of time spent online. This year the survey included additional questions exploring children's and parents' perceptions of the OSA, and this survey data was combined with qualitative research which forms the basis of this report.

Quantitative Research

Research is based on an online survey of 1,270 UK children aged between 9 and 16 and their parents. The report focuses on questions relating to the OSA, while a previous report details findings from the main survey.[iii] The fieldwork for this research was conducted between 15th September and 1st October 2025, which was relatively soon after the OSA's Protection of Children Codes had come into force on 25th July 2025. Whilst questions often referenced 'recently' or 'in the past two months', survey respondents, because of natural recall, may have been thinking about periods before the Protection of Children Codes came into force. Similarly, impacts linked directly to the OSA may not yet be fully realised at the time of this research.

The survey was completed online with parents who had at least one child aged between 9 and 16. Parents were first asked to answer a set of questions on the use of digital technology in relation to one of their children. The survey was then handed over to their child to answer a similar set of questions.

Quotas in line with ONS population estimates were put in place to ensure the sample was stratified by each age group, with equal representation of boys and girls at each age. This is in line with the approach taken in previous waves, with the targets of boys and girls at each age in line with UK population estimates.

Weighting

The sample was weighted to ensure representativeness with the broader population of UK children. Targets were gender, age, region and the Index of Multiple Deprivation, as well as parent gender.

Statistical significance

All comparison statistics highlighted in this report, including between subgroups, are statistically significant at the 95% confidence level. This means that the observed differences are highly unlikely to be due to chance and instead reflect genuine changes or trends.

Qualitative Research

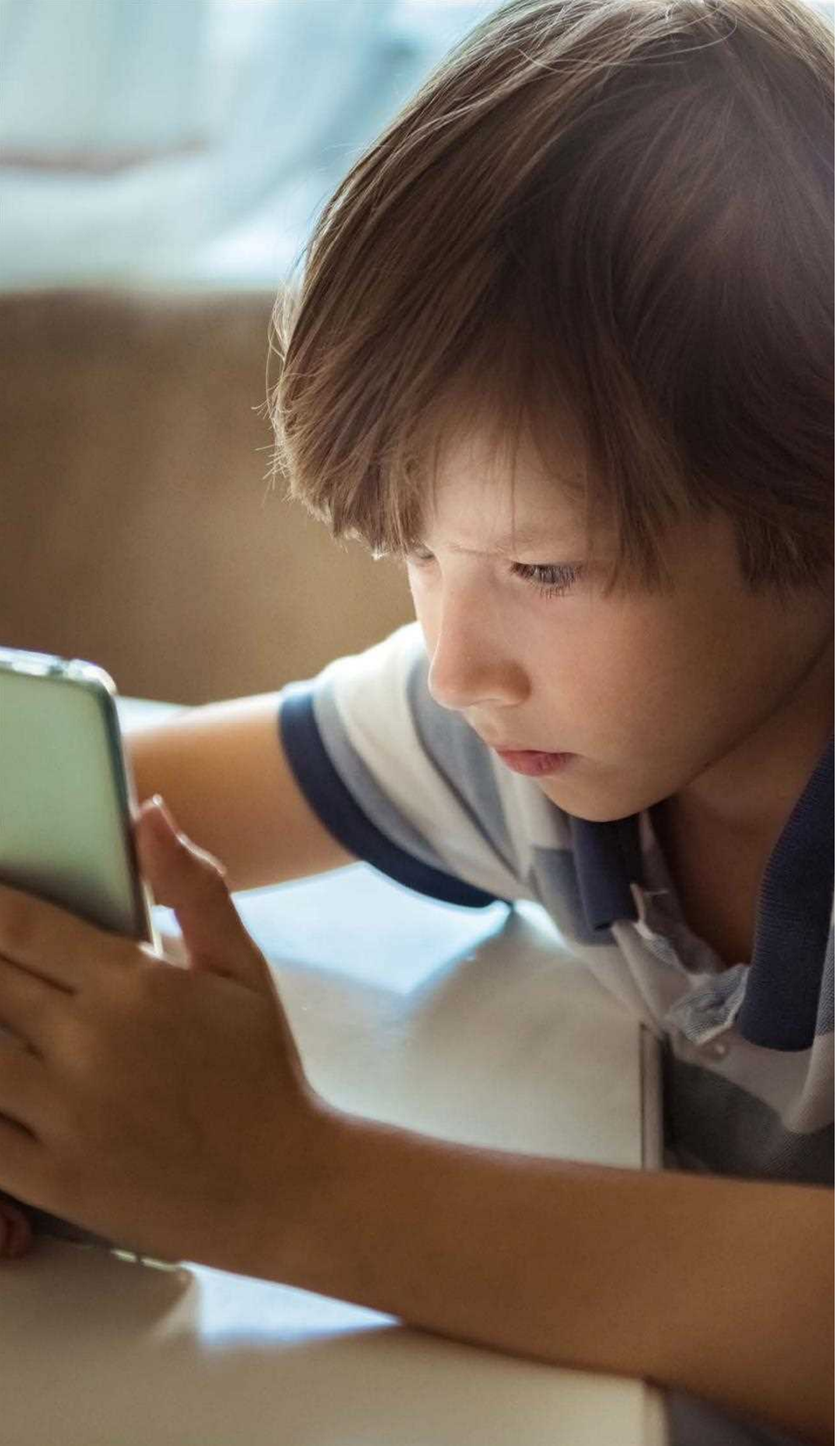
Seven focus groups took place between 2nd and 16th February 2026. Four of these were with children aged 11-16 and three with parents or guardians of children aged 11-16. Each focus group was mixed gender, though groups were split by age, for example 11–12-year-olds were grouped together.

Children's focus groups lasted up to 75 minutes, and adult groups up to 90 minutes. Meetings took place virtually on Zoom, with participants having been recruited by a trusted partner agency. Participants were paid as a thank you for their time.

Questions centred around changes that children and parents have seen in the online world recently, how they felt about them, and how these changes have impacted their perceptions of children's safety online. Discussions also examined what changes to legislation were effective in improving online safety, and what alternative ideas they had for keeping children safe online.

Sample breakdown

Method	Sample definition	n.
Panel survey	Children aged 9-16 and their parents	1,270
Focus groups	Children aged 11-12	6
	Children aged 13-14	12
	Children aged 15-16	5
	Parents of children aged 11-12	8
	Parents of children aged 13-14	6
	Parents of children aged 15-16	7



Background:
What is the Online Safety Act?

After a long passage through Parliament, the Online Safety Act (OSA) became law on 26 October 2023. The Act was intended to make the UK "the safest place in the world to be online" by holding online services accountable for the safety of their users.[iv] While it tackles a wide range of online issues – from the circulation of illegal content to user empowerment features – protecting children is a central focus.

The Act covers many online spaces including user-to-user services, search platforms and pornography providers, with factors like the size of a platform's user base and the risks it poses determining which specific aspects of the Act apply. However, a key criticism of the Act is its ability to respond quickly to new and emerging technologies, particularly generative AI.[v] These systems do not always fit neatly within existing categories, raising questions about how effectively they are captured by the current regulatory framework.

A primary focus of the Act is protecting users from harmful content. It requires companies to protect all users from illegal content – such as terrorist material or content encouraging self-harm, as set out in the Illegal Harms Codes.[vi]

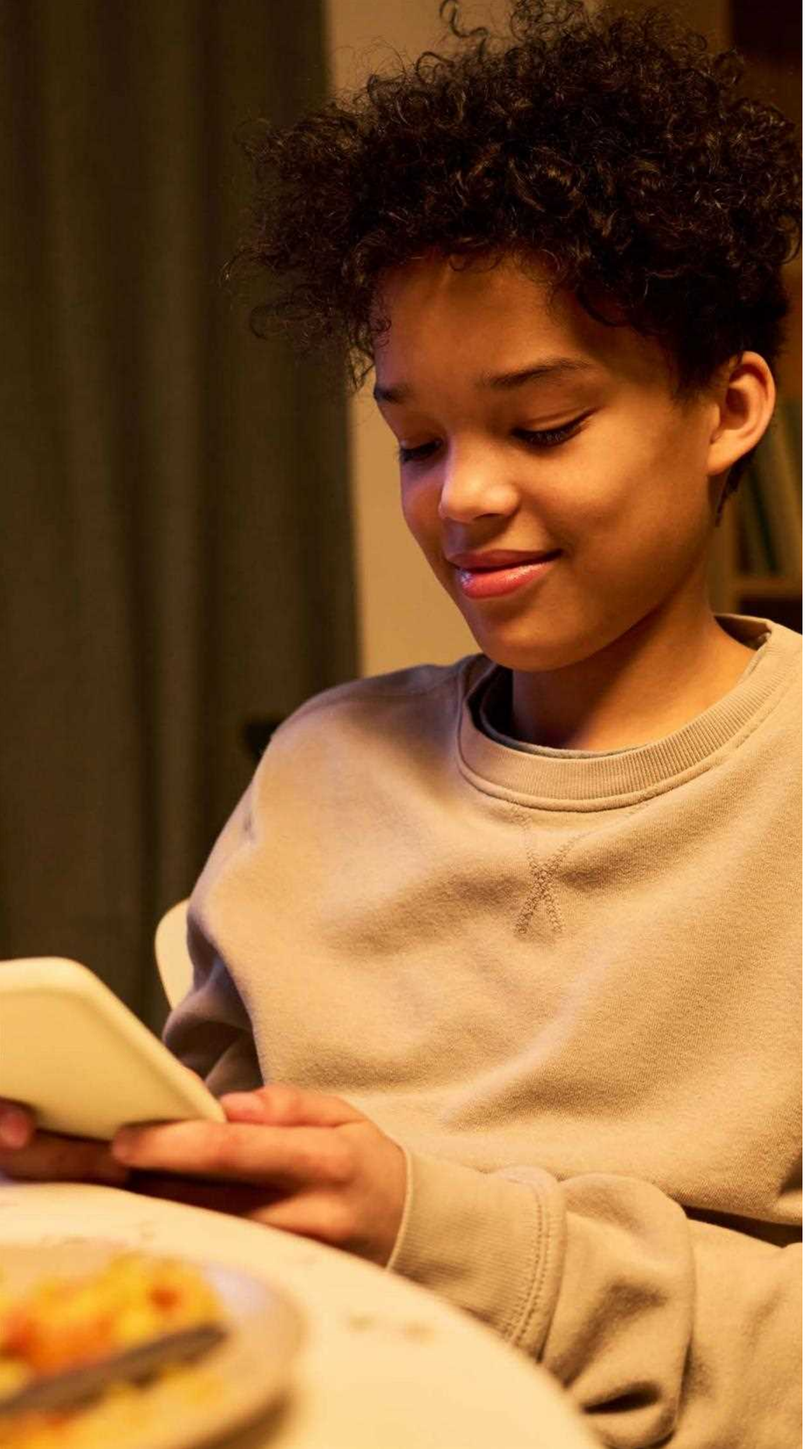
The Act also introduces additional protections for children through the Protection of Children Codes (hereafter the Children's Safety Codes), which came into force on 25 July 2025.[vii] These require relevant services, including social media and gaming platforms, to:

- Identify and assess risks to children from content and features
- Take proportionate action to mitigate exposure to content that is legal but harmful to children, such as eating disorder or hateful content
- Provide age-appropriate tools and settings, such as clear reporting mechanisms, content filters and prompts to help children manage their experience
- Ensure terms, policies, and safety information are accessible and understandable for children

In addition, the Act also requires services hosting pornographic content to implement highly effective age assurance, to prevent children from accessing such material.

Ofcom, as the UK's online safety regulator, is the independent body responsible for implementing and enforcing the Act. When companies fail to comply, Ofcom can issue fines or take business disruption measures. As of March 2026, Ofcom had issued 16 fines totalling nearly £4 million.[viii]

This report explores the early impact of this legislation on families.



Section 1: Children's online spaces: *the visibility of new safety features*

The OSA is making safety features more visible across children's online spaces, with parents and children largely welcoming these changes. Families report more frequent age checks, clearer content warnings, improved reporting tools, and enhanced parental controls.

Parents and children are aware of new rules to keep children safer online

Most parents say they are aware of the OSA, with 68% reporting they had heard of the Act and 27% saying they have not. Despite this, parents' understanding of the legislation is limited, with many unsure what the Act specifically does beyond relating to online safety. When discussing the new rules with parents, they were broadly positive, but as this report discusses, many are sceptical about their impact.

Although children were not familiar with the OSA by name, some reported hearing about new rules and related changes, most often at school. Children were generally positive about measures aimed at improving their online experience, although many doubted whether they would have a meaningful impact.

Mum of boy, 16

"I'm definitely supportive [of new rules] but what worries me is how effective they can really be."

Mum of boy, 16

"To me they seem a bit more of a tick box rather than a restriction or to make things better."

Dad of girl, 11

"I think I've heard of it vaguely, but I don't know what all the terms and policies are."

Seven in ten parents and children have noticed changes to online spaces

Age checks and new safety tools and functions are increasingly visible online, with two-thirds (67%) of parents reporting noticing changes to their child's online accounts. These include children being asked to prove their age to use a platform (29%), seeing easier ways to block or report content or users (25%) and more content warnings or filters (21%), although parents do not necessarily link these to the OSA.

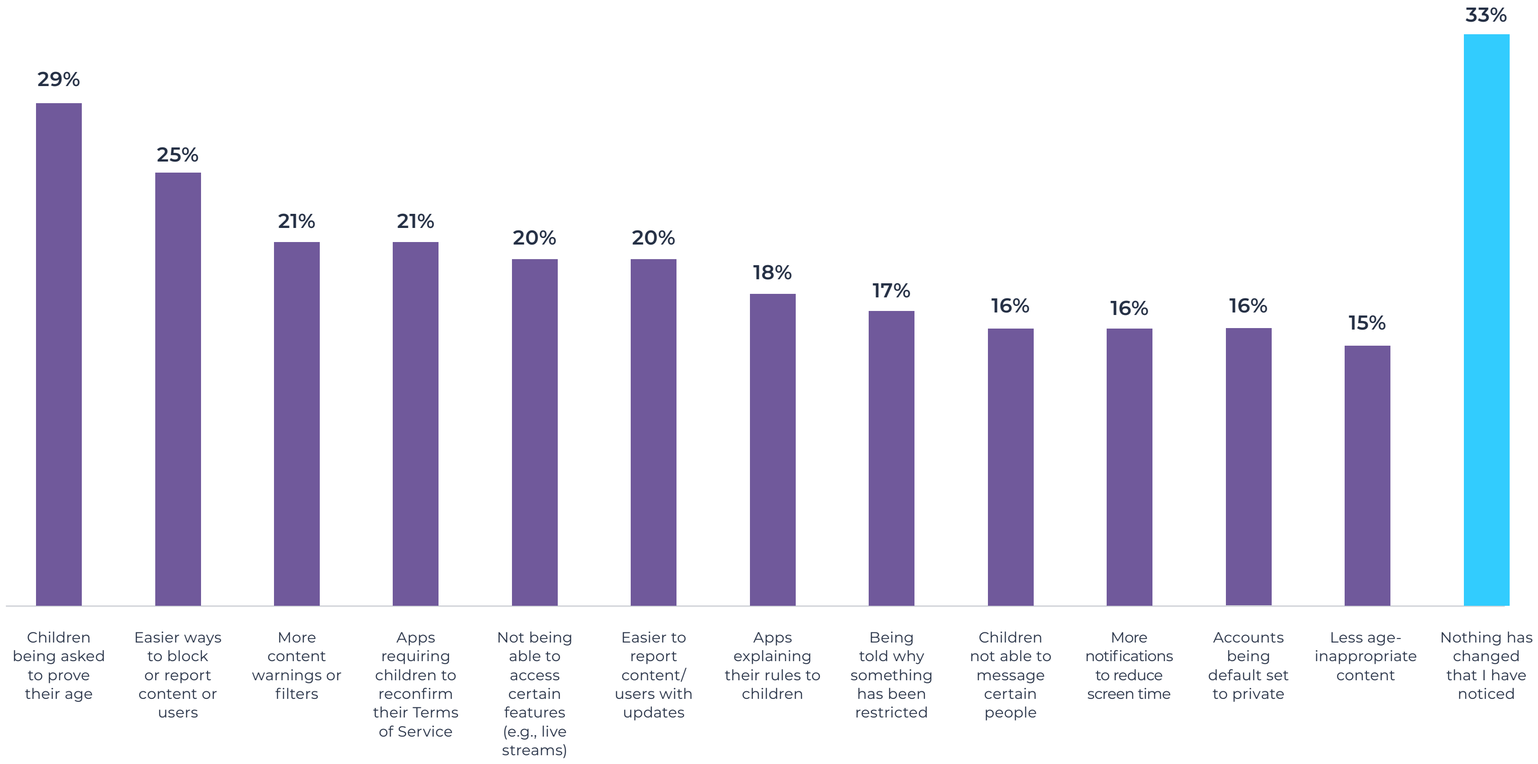
Dad of boy, 15

"[I've noticed more] restrictions for content mainly. There are generally warnings beforehand."

Mum of girl, 11

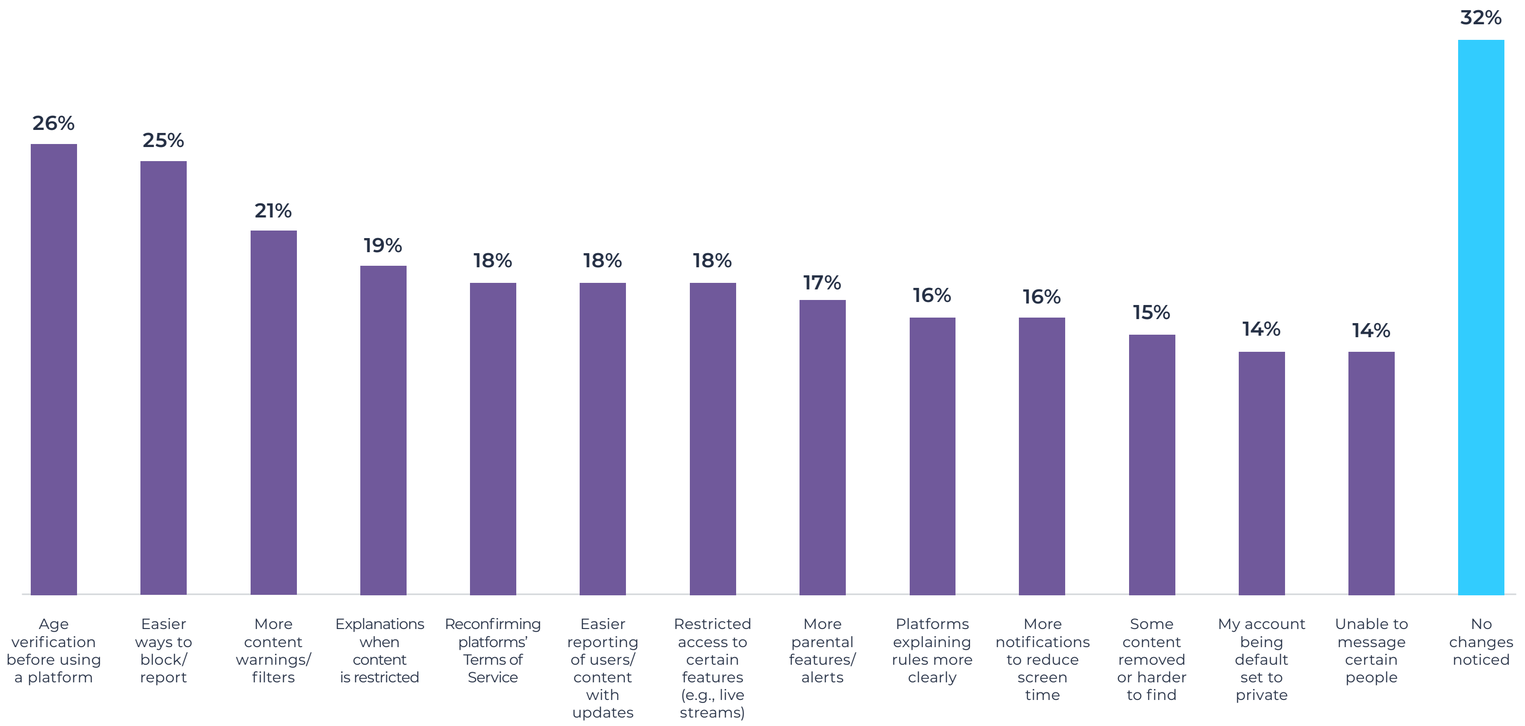
"I think TikTok has put an age restriction in, and they've actually got to verify that they're 13 or over now."

Figure 1. Seven in ten parents have noticed changes to online spaces:
Recent changes on websites or apps noticed by parents on children's accounts



QOSAP5A. Have you noticed any of the following changes on the online accounts belonging to your <age> year old <son/daughter> recently?
Base: 1,270 parents of children aged between 9-16. Text in response codes have been lightly edited for presentation purposes.

Figure 2. Seven in ten children have noticed changes to online spaces:
Recent changes in websites or apps noticed by children on their accounts



QOSAC3. Have you noticed any of the following on the apps, platforms or websites you use recently?
Base: 1,270 children aged between 9-16. Text in response codes have been lightly edited for presentation purposes.

Similarly, 68% of children have noticed changes to the apps, platforms or websites they use. The most common changes they have noticed are being asked to prove their age before using a platform (26%), easier ways to block or report users or content (25%) and more content warnings (21%).

In focus groups, children discussed the changes they noticed in terms of what they can and cannot do online. These discussions included mentions of age checks blocking them from using platforms or functions such as livestreaming, and stricter rules about who they can chat to or share things (such as their location) with.

Boy, 14

"I don't think it's a bad thing, except I don't think it makes a huge difference."

Girl, 14

"Lots of my friends on TikTok have age restrictions on their profile, so they can't message people or share videos with them."

Parents value enhanced parental controls but see their limits

Nearly two-thirds (64%) of parents say they have noticed recent changes to parental controls. These are spread across different features, with a quarter (25%) noticing more screen time controls, new ways to limit age-inappropriate content, or more ways to manage their child's privacy settings. While providing parental controls is not a requirement for platforms under the Act, many have enhanced these features as part of broader child safety updates.

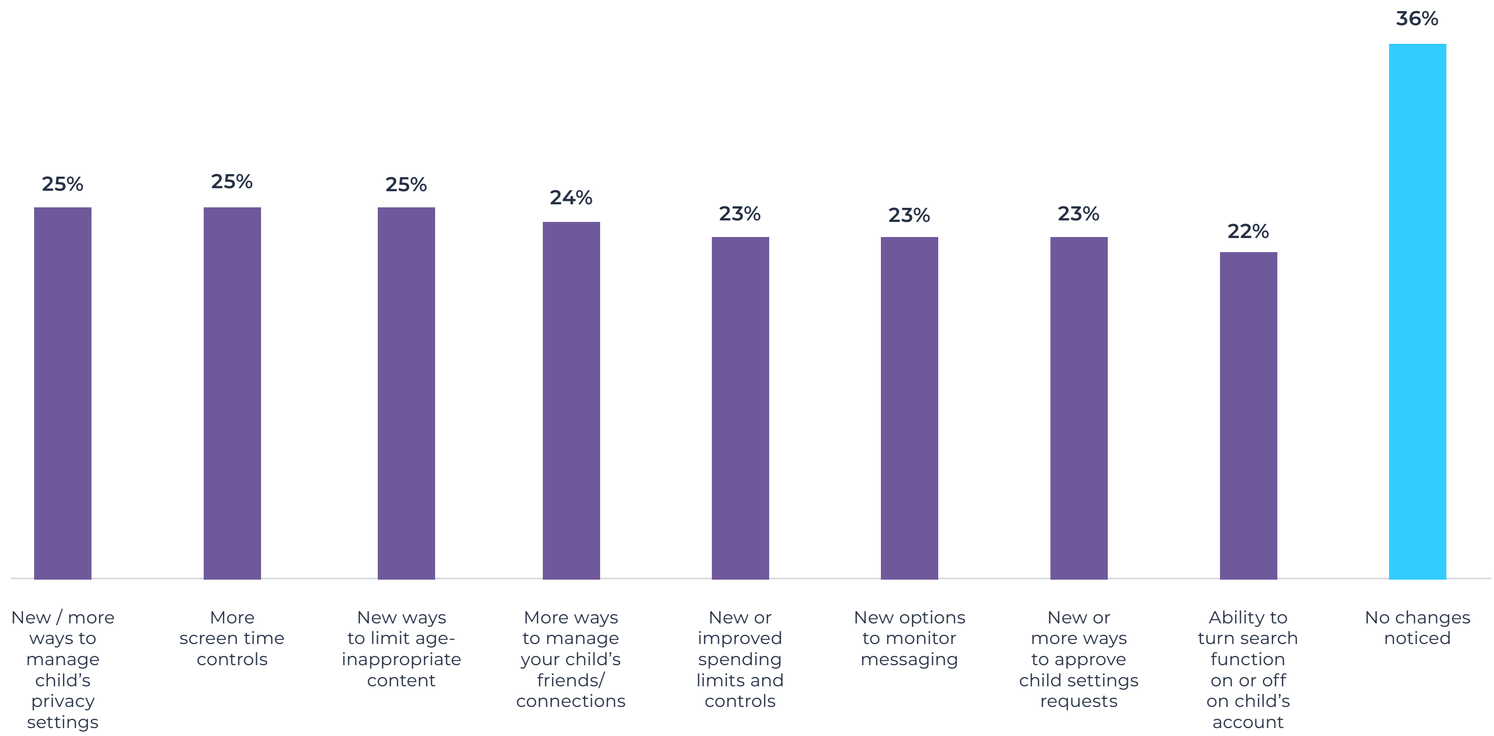
Parents welcome improved parental controls and highlighted the many ways in which they use them to manage their child's online activities, from limiting screen time to controlling who can contact them. However, they also recognise that these measures alone are not enough to keep children safe online.

It is promising that both parents and children have noticed safety changes to children's online accounts, and that sentiment towards these updates is positive. Yet these changes alone may not be enough if they do not lead to tangible improvements in children's online safety and digital wellbeing. The following sections examine whether these changes have been effective and their impact.

Dad of girl, 14

"It could be a full-time job for you to police what platform they're on, what they're looking at, how they get around it."

Figure 3. Parents value enhanced parental controls: Changes to parental controls parents have noticed



QOSAP6. Have you noticed any of the following changes to parental control features on the online accounts belonging to your <age> year old <son/daughter> recently?
Base: 1,270 parents of children aged between 9-16

Section 2:
Age verification:
effectiveness in practice

Age checks are a central part of keeping children safe online, by helping platforms understand the age of their users so that content, features and interactions can be tailored appropriately. When implemented effectively, age checks place the responsibility on platforms – not parents – to ensure children are accessing age-appropriate content and features.

Encouragingly, children are being asked to age verify more in online spaces. However, these age checks are not always effective, with children speaking confidently about bypassing them – sometimes with the support of their parents.

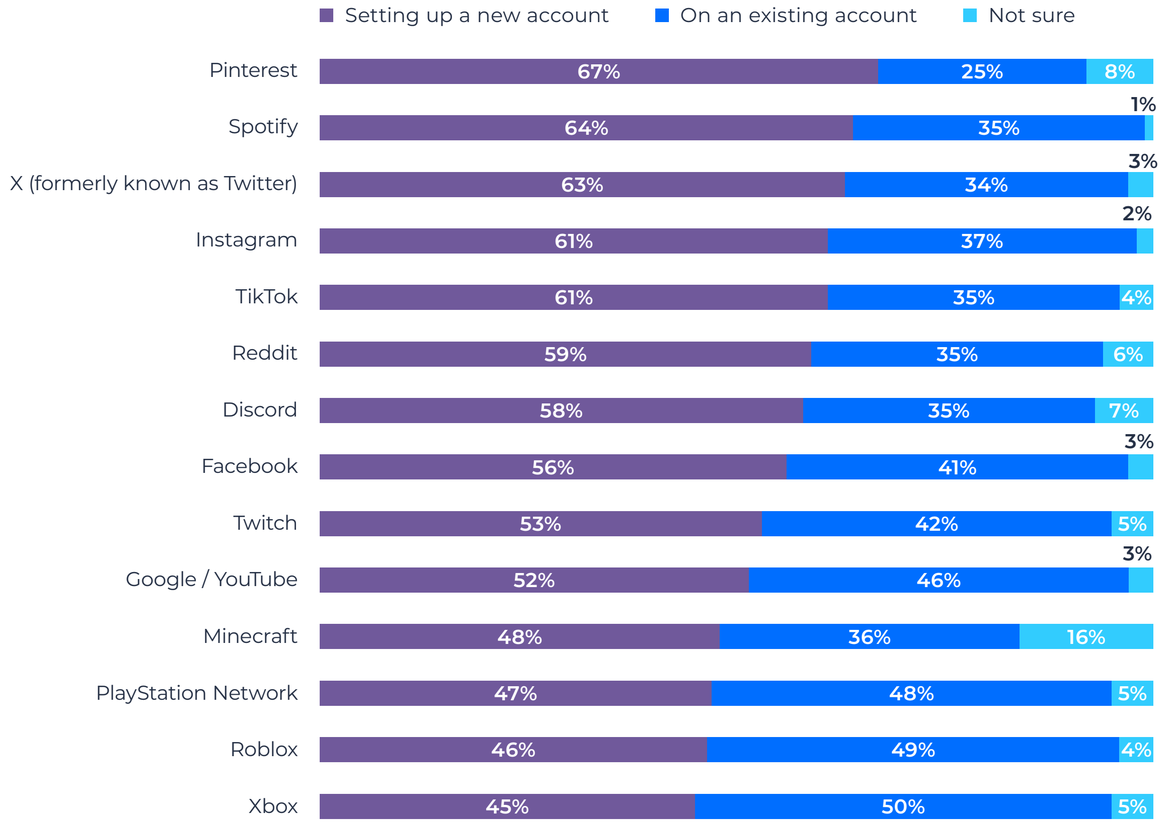
Children are being asked to age verify online – on a range of platforms

53% of children reported being asked to verify their age online[3] in a two-month period.[4] Encouragingly, these age checks are taking place on a range of platforms, across both new and existing accounts. Popular platforms and websites where children had been asked to age verify recently included TikTok (34%), Google/YouTube (26%), and Roblox (17%).

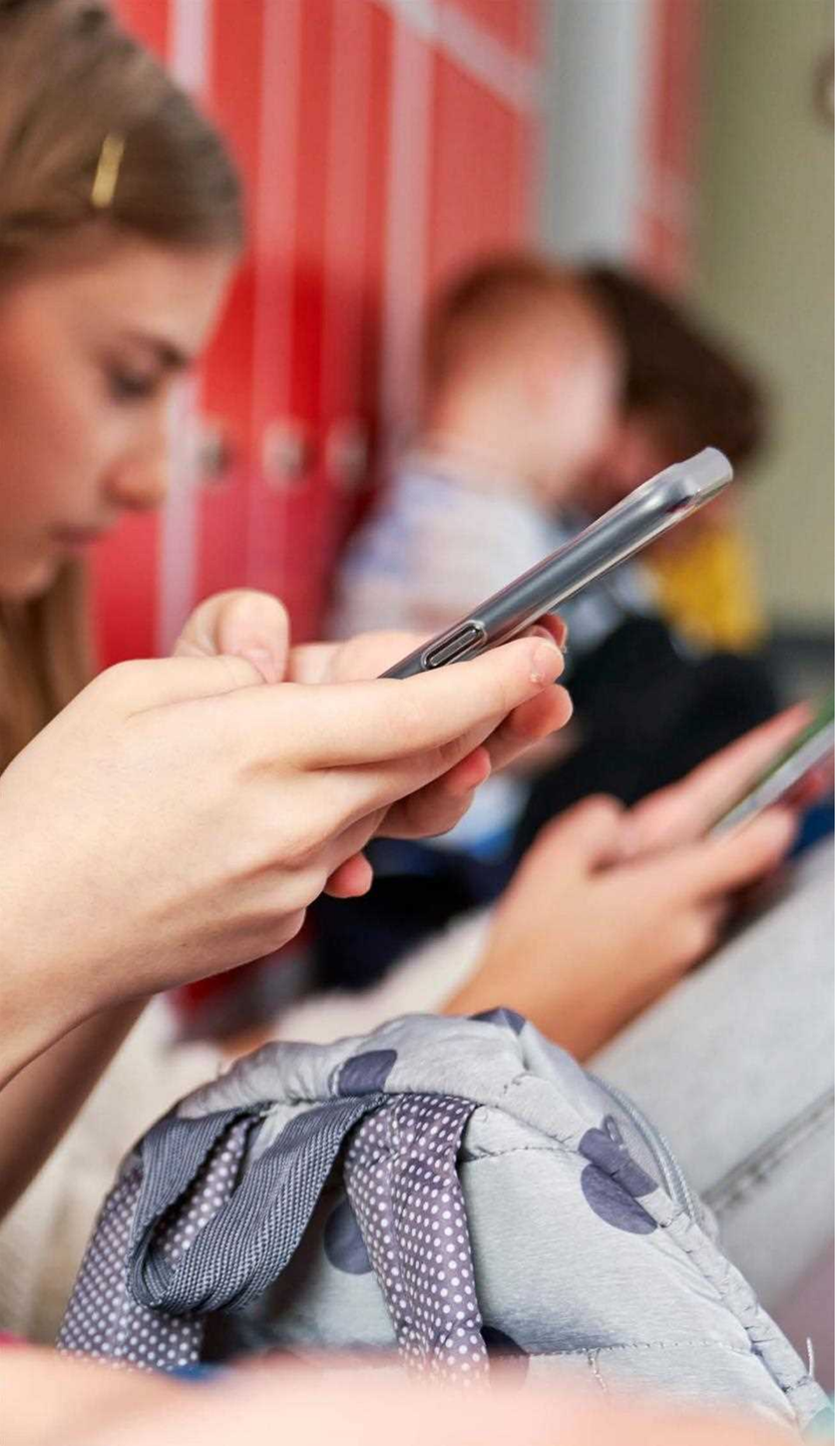
For most children, age verification happened when setting up a new account (55% on average), while 39% were asked on an existing account.[5] It is important that children are asked across both new and existing accounts as many have previously set up accounts below the minimum age.[ix] Verifying existing accounts helps prevent underage use and age-inappropriate experiences.

3. *When asking children and parents about their experiences with age verifying, we asked them to think about a range of methods, some of which are not considered highly effective (such as entering a fake birthdate).*
4. *As the survey was conducted September – October 2025, the two-month period we asked children about refers to approximately mid-July – end-September 2025.*
5. *Children were asked which platforms they were asked to age verify on and whether this was on a new or existing account. The average has been calculated as the mean percentage score across all platforms.*

Figure 4. Children are being asked to age verify on a range of platforms:
Whether child was asked on a new or existing account



QOSAC6. For each of these platforms were you trying to set up a new account or were you on an existing account?
Base: Floating base where child has been asked to age verify on platforms



A range of age verification methods are being used

Where children encountered age verification, 37% report using facial age recognition, while others verified their age through a third-party app (24%) or government ID (22%). Notably, a third (34%) of children chose not to complete the verification process when prompted. Some reasons given for this included it being too much effort, or because the process made them realise the content was for older audiences, so they stopped trying.

Promisingly, most methods of age verification were seen as easy for children to complete. According to all children, the following methods were described as easy: uploading a government ID document (88%), facial age estimation (89%) and using a third-party app (88%).

Children and parents are supportive of age verification online

Children and parents were generally positive about age verification. Children understood that these checks exist to support their safety and accepted that being unable to access certain content or features on a platform likely meant it was not suitable for them. Meanwhile parents saw age checks as a useful way to restrict children's access to inappropriate content and contact, and supported wider roll out.

We also asked parents specifically whether they support age verification as a way to prevent children from accessing pornography. Support for this measure was strong, with 84% of parents in favour of using age checks to restrict access to pornographic content.

Girl, 13

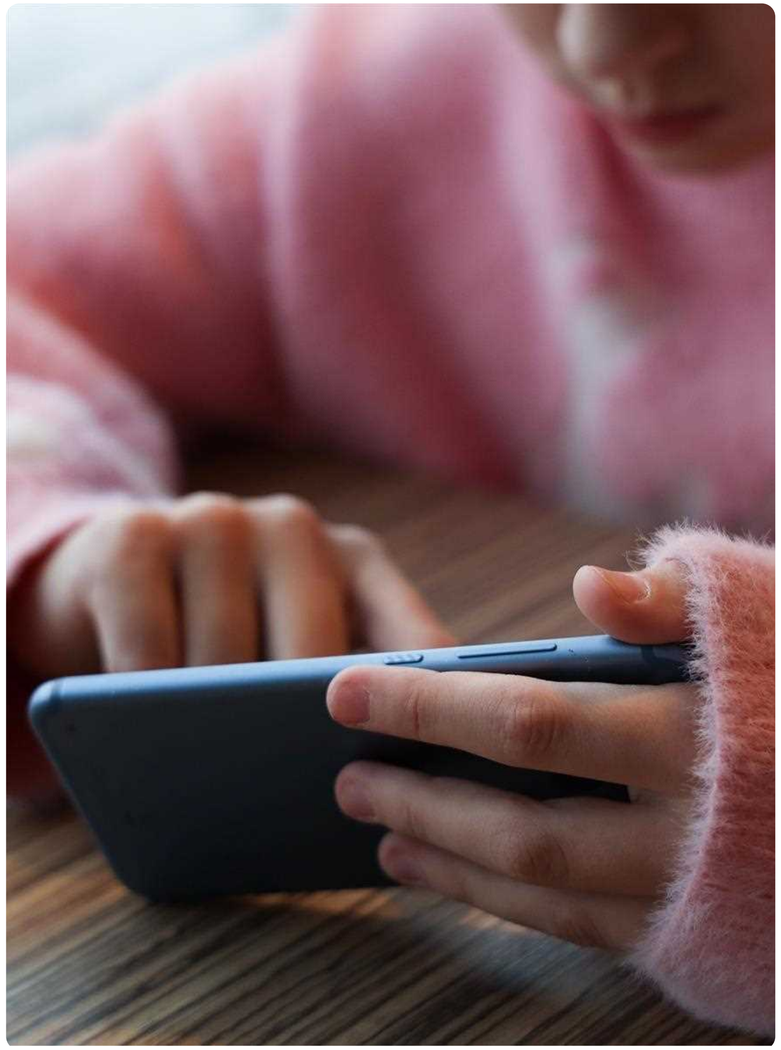
"I think it's good [age verification] so people not the right age can't get onto like, gambling stuff."

Mum of boy, 12

"I'm always checking to see who he's speaking to, and how does he know they are the age they say they are?"

Girl, 14

"I just scroll past it [age verification]. If it's not made for a certain age group, then there's no point."



Despite high support, parents and children still had concerns about the use of age verification

One concern around age verification was data protection. Some children and parents felt uncomfortable sharing personal information (such as passport details) online and preferred using facial videos instead. Others had hesitations about biometric videos fearing their data could be used for other purposes. Previous research by Internet Matters found that the most common concern amongst parents and children relating to online age verification was privacy and how their data may be used.[x]

Willingness to share data also varied depending on the trust parents and children had in the platform, app or website involved. However, no one said they would rule out submitting information completely, and some noted that just by being online you are sharing your data with platforms.

Dad of girl, 11

"Kids don't know the difference between a genuine website and a website that isn't genuine. If all websites have facial verifications and they go on a website that is not genuine, their face and their documents could be used to do illegal stuff."

Parents are also concerned about age checks being bypassed

Nearly two-thirds (62%) of parents say they are concerned about their child bypassing age verification measures. This concern decreases as children get older, with parents of 15 and 16-year-olds being significantly less likely to be concerned (40%). Meanwhile, parents of vulnerable children are more likely to be concerned than parents of children without these vulnerabilities (73% cf. 57%).[6]

Mum of girl, 12

"I don't class [age verification] as being a deterrent. If anything, because they've had a barrier put up, kids will do everything they can to be the first one to get through it."

Boy, 13

"It depends on what site, if you trust it or not. If it's a trusted platform where it's encrypted, probably."

6. *Throughout the report we refer to children who have an Education, Health and Care Plan (EHCP), who receive special educational needs (SEN) support, and/or who have a physical/mental health condition which requires professional help, as 'vulnerable' or as 'children with vulnerabilities'. We recognise that there are multiple understandings of the term vulnerable, and this definition is for the purpose of this report.*

Age checks are widely perceived by children as easy to bypass

This concern is not unfounded, as 46% of children believe age checks are easy to bypass, while only 17% say it is difficult. Older children are more likely to think they are easy to bypass than younger, with 52% of those aged 13 and over thinking they are easy compared with 41% of those aged 12 and under.

In focus groups, children demonstrated a clear awareness of how to bypass age checks, either through their own experiences or by hearing about methods from others. Methods ranged from simple approaches, such as entering a different birthday, to more sophisticated methods including using someone else's ID or submitting a video of another person's face – or even a character – to trick platforms into estimating an older age. Using a Virtual Private Network (VPN) was mentioned in a handful of cases, however, they were not among the most discussed methods for bypassing age checks. Parents were also aware of the ease with which age checks can be bypassed.

One technique brought up was children drawing facial hair on themselves so that the tools verifying them would think they were older, which was reported as working in multiple instances.

Girl, 11

"I've seen clips of people online where they'll get clips of video game characters like turning their head and use it for age verification"

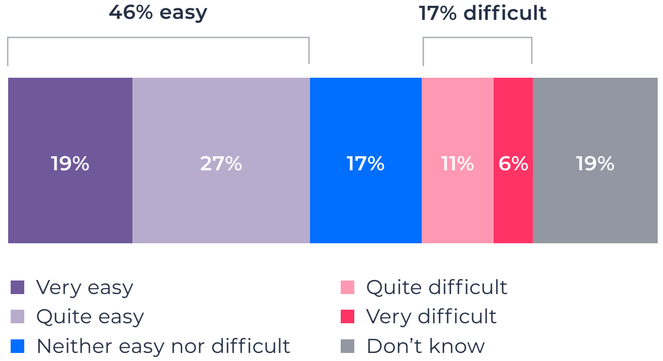
Mum of boy, 12

"I did catch my son using an eyebrow pencil to draw a moustache on his face, and it verified him as 15 years old."

Boy, 13

"If [going live] needed an ID, I'd use my parent's ID and then if they wanted to upload a photo, I'd go online and upload any."

Figure 5. Widespread perception that age checks are easy to bypass: How easy or difficult it is to get past age verification according to children



QOSAC9. How easy or difficult do you think it is to get past age verification?
Base: 1,270 children aged between 9-16

Dad of girl, 11

"I think there's still probably pretty easy ways around [age verification]. There are lots and lots of different ways you can use AI to make your face look older."

Children also reported that even where they were honest, age verification technologies used by platforms were not always effective, with some misjudging the age of a face. Where this happened, children acknowledged continuing to use the platform with the wrongly estimated age. While others mentioned that even when they were correctly identified as being too young, little was done to prevent them trying again.

There was also concern among both children and parents that age verification tools could be misused by adults – putting children at risk. Some participants had heard of cases where adults use images or videos of children to gain access to spaces intended for younger users. This is concern is borne out in recent media reports of adults purchasing or obtaining accounts registered to children for this purpose.[xi]

Boy, 12

"On Roblox there's a thing where you put your face in and only allowed to chat with that age group... I got 15 when I'm 12, so I'm chatting with people older than me when I shouldn't be."

A third of children say they have circumvented age checks

Not only are age checks perceived as easy to bypass but a third (32%) of children admit to having done so in the past two months. Older children are slightly more likely to report bypassing age checks, with 35% of those aged 13 and older reporting they have done so, compared with 29% of those aged 12 and under.

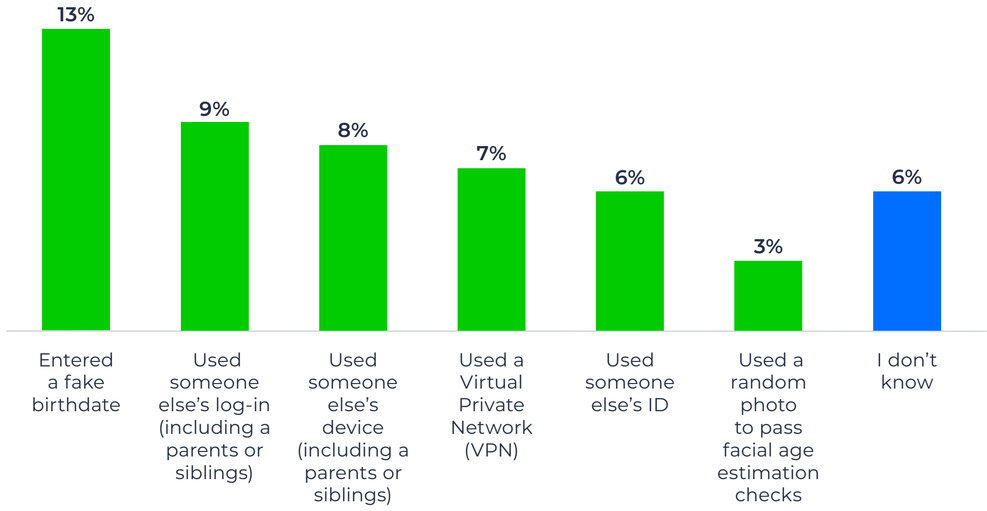
Notably, children who bypass age limits are less likely to discuss their online activities with their parents. Among those who do not discuss their activity, 37% have bypassed restrictions, compared with 26% of children who do. This suggests that open communication may encourage safer and more responsible online behaviour.

To get around age restrictions, children use a wide variety of methods. With some of the most common being entering a fake birthday (13%), using someone else's login (9%) and using someone else's device (8%).

Non-binary child, 13

"Adults can very easily use a face they searched on the internet to trick it into thinking you're someone you're not – so there might be adults in kids age groups trying to groom them."

Figure 6. Common ways children circumvent age restrictions:
Methods children have used in the past two month to access features, apps or platforms that are age restricted



QOSAC8A.1. Have you or any of your friends/peers done any of the following to access features, apps, platforms or websites that you're limited from using due to your age in the past 2 months? - Me
Base: 1,270 children aged between 9-16

Girl, 12

"Every time I go live on TikTok, it tells me I have to be 18, but when the AI detects that I'm not 18 they ban me. But they only ban me for 10 minutes and then I can go live again."

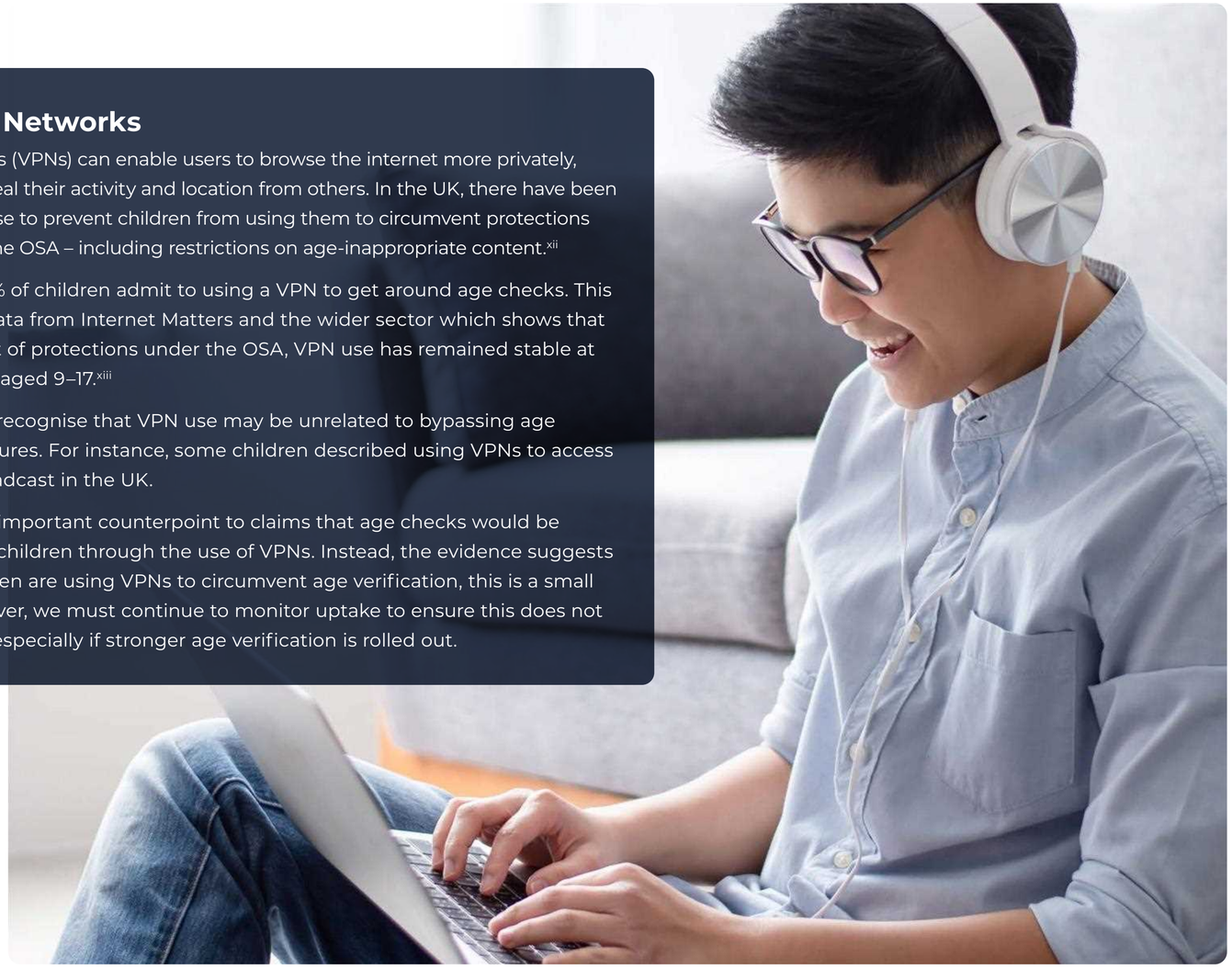
Virtual Private Networks

Virtual private networks (VPNs) can enable users to browse the internet more privately, allowing them to conceal their activity and location from others. In the UK, there have been calls to regulate VPN use to prevent children from using them to circumvent protections introduced as part of the OSA – including restrictions on age-inappropriate content.[xii]

Encouragingly, only 7% of children admit to using a VPN to get around age checks. This aligns with previous data from Internet Matters and the wider sector which shows that since the enforcement of protections under the OSA, VPN use has remained stable at around 8% of children aged 9–17.[xiii]

It is also important to recognise that VPN use may be unrelated to bypassing age checks or safety measures. For instance, some children described using VPNs to access sports games not broadcast in the UK.

These findings are an important counterpoint to claims that age checks would be easily sidestepped by children through the use of VPNs. Instead, the evidence suggests that while some children are using VPNs to circumvent age verification, this is a small number overall. However, we must continue to monitor uptake to ensure this does not change in the future, especially if stronger age verification is rolled out.



The most common reasons children gave for circumventing age checks were to access a social media platform they were not old enough to use (34%), followed by to join an online game or gaming community (30%) and to use a chat or messaging app (29%).

The data shows that the method of circumvention children use tends to vary depending on the type of content or activity they are trying to access. For example, 38% of children entered a fake birthdate to access a platform they were not old enough to use, compared to only 9% using this method to access a forum or discussion board as shown in Figure 7 on the next page.

The reasons for this are likely multi-faceted. In some cases, it may reflect the strength of age assurance measures in place. Where platforms contain content that is subject to more robust verification (such as self-harm or pornographic material), children may be more likely to use methods such as VPNs or someone else's ID, as they are more effective at bypassing these controls. By contrast, platforms with a lower barrier to entry, such as gaming or social media, mean that simpler methods like entering a false date of birth may be enough to gain access. In other cases, the choice of method may be influenced by a desire to avoid detection, with children opting for approaches that feel more anonymous or less likely to be traced.

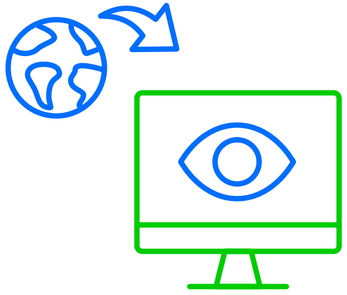
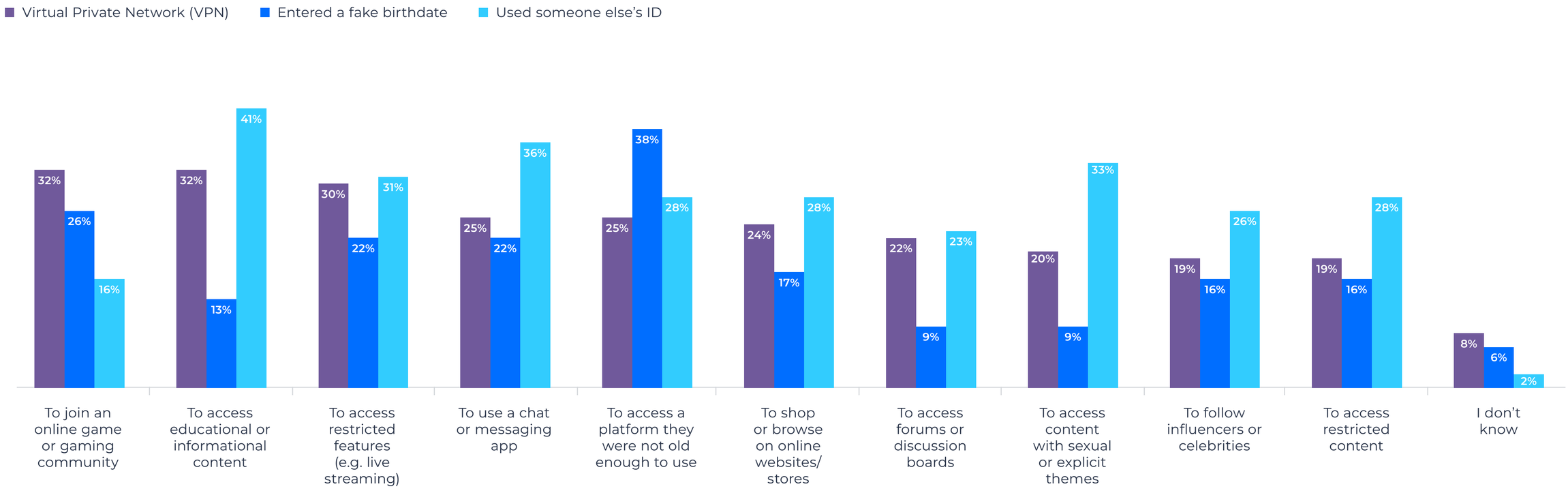


Figure 7. Children bypass age verification for a range of reasons: Content children were trying to access by age circumvention method

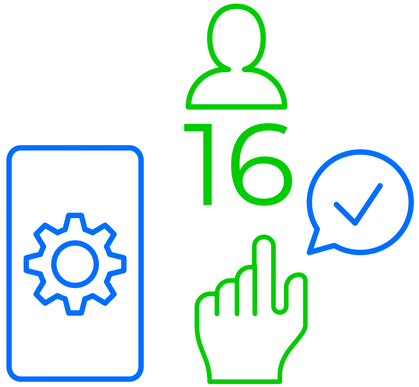


QOSAC8B. What were you trying to do when you...?
Base: Floating bases of those who have circumvented age assurance using different measures

One in six parents have helped their child bypass an age check

A quarter (26%) of parents have allowed their child to bypass age checks, with 17% actively helping their children and 9% allowing it or "turning a blind eye". When speaking to parents and children about these situations, they described scenarios in which parents felt they understood the risks involved and based on their knowledge of their child, were confident the activity was safe. Examples included allowing a child to go live on TikTok when the parent knew who would be watching, or permitting access to certain games that the parent had previously played and considered appropriate for their child's maturity.

Given widespread awareness – and in some cases experience – of bypassing age checks, it was generally acknowledged that, while age verification measures are positive, they are not always accurate or stringent in practice. This is concerning because without robust verification and enforcement, children may continue to access content and features that are unsuitable for them, leaving the burden of protection largely on parents and carers. If age verification is to be used to keep children safe online, then platforms, government and the regulator need to ensure it is effective.

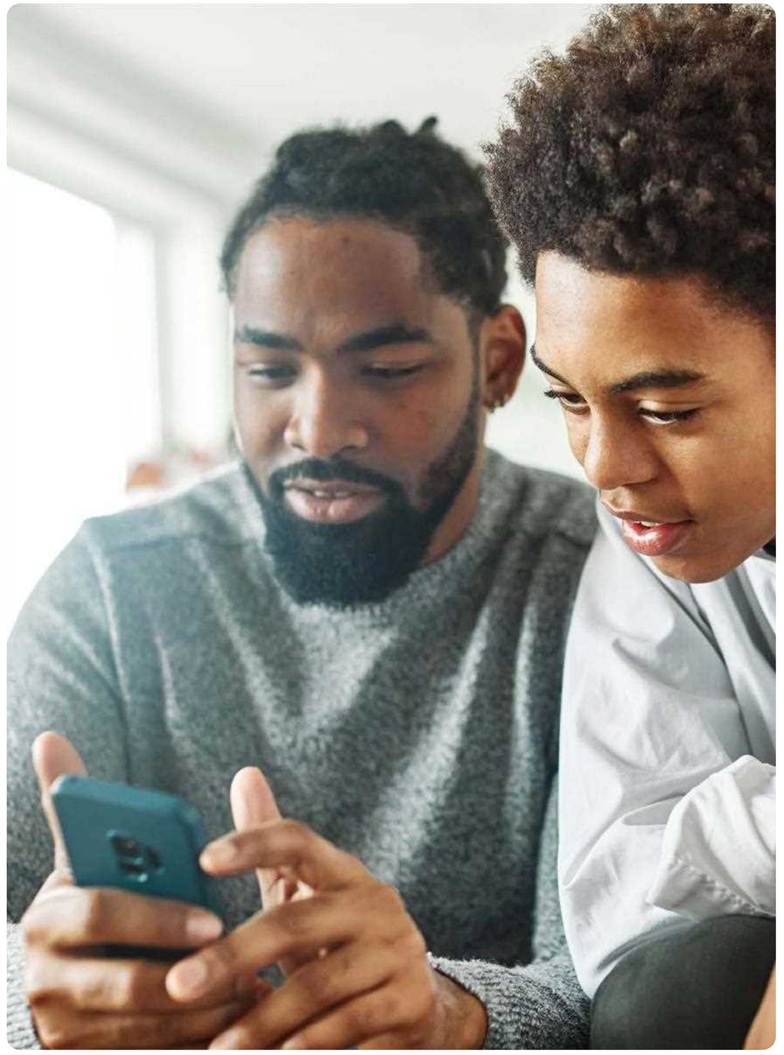


Mum of non-binary child, 13

"I have helped my son get around them. It was to play a game, and I knew the game, and I was happy and confident that I was fine with him playing it."

Girl, 12

"I have one account on TikTok I go live on, so I got my mum to put her ID in. She says it's because she trusts me. I don't show my face on it so I don't get banned."



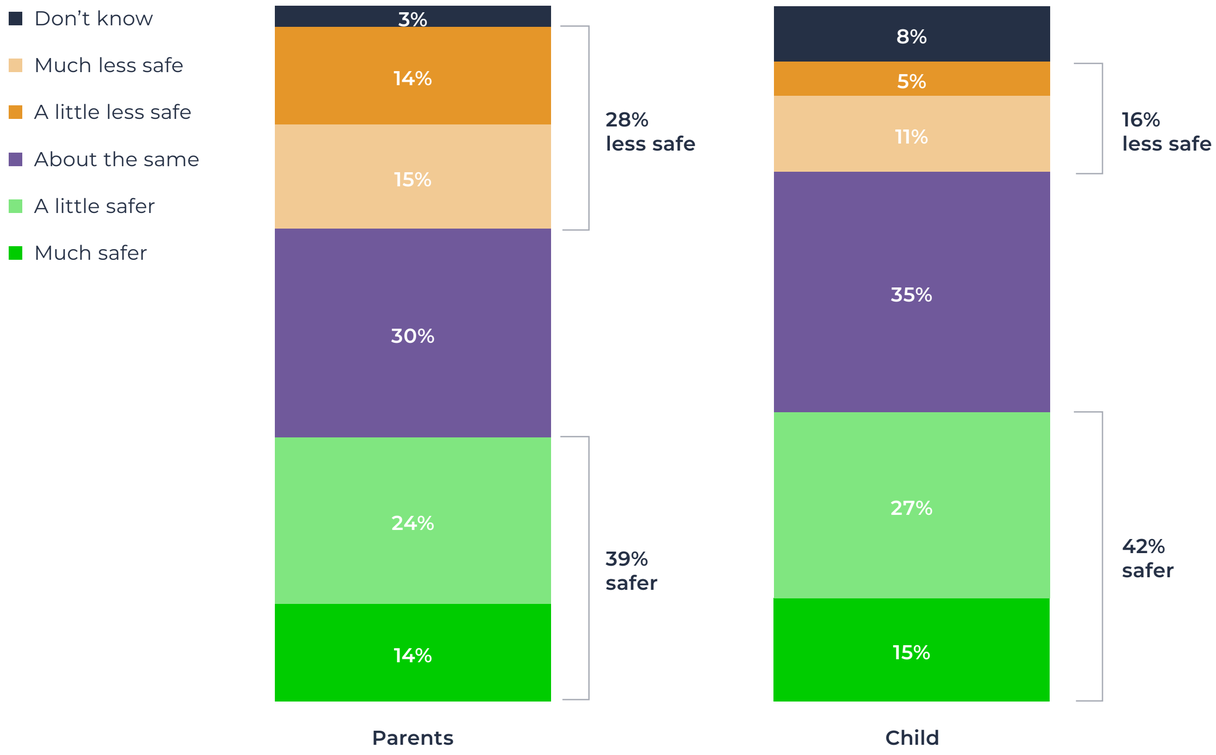
Section 3:
Changing online experiences:
progress and gaps

Children who have noticed new online safety measures view these changes positively, particularly restrictions on stranger contact and improved platform reporting tools. Many also report encountering more age-appropriate content online. This is likely why some feel the online world is getting safer for them. However, with children continuing to encounter harm at high rates, there is still progress to be made. Parents and children also express concern about risks that fall outside the scope of existing legislation, including excessive time spent online and the growing presence of AI-generated content.

Mixed views on children's online safety

Parents are divided on whether the online world is getting safer for children. While 39% feel the online world has become safer recently, 28% feel it has become less safe. Among children, 42% see the online world as becoming safer for them, compared to 16% who think it has become less safe.

Figure 8. Parents and children are optimistic the online world is becoming safer:
Parents and children's views on whether online world has become safer for children recently



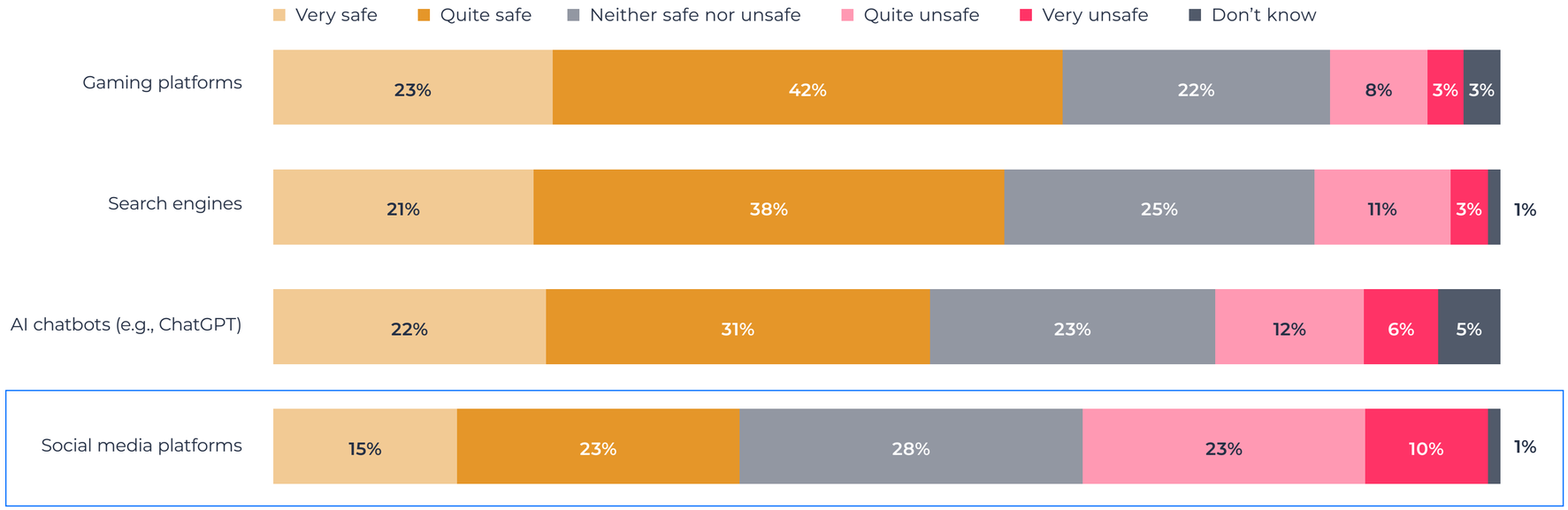
QOSAC2. Do you think the online world has become more safe or less safe for you and other children like you recently /QOSAP4B. Do you think the online world has become more safe or less safe for your <age> year old <son/daughter> recently? Base:1,270 parents of children aged 9-16 / children aged 9-16

Parents view social media platforms as less safe for children than other online spaces

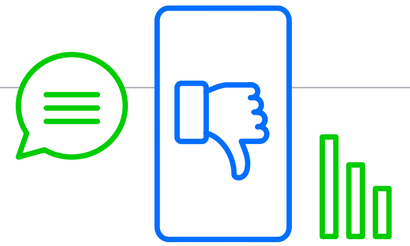
One reason for these differing views amongst parents may be the online spaces children use, with perceptions of safety varying by platform type. Parents generally view gaming platforms, search engines and AI chatbots as safe spaces, with 64%, 59% and 53% respectively viewing them as safe, compared with 11%, 15% and 18% viewing them as unsafe. Compared to these other spaces, parents are a lot less likely to view social media as safe (37%) and are more likely to view it as unsafe (33%).

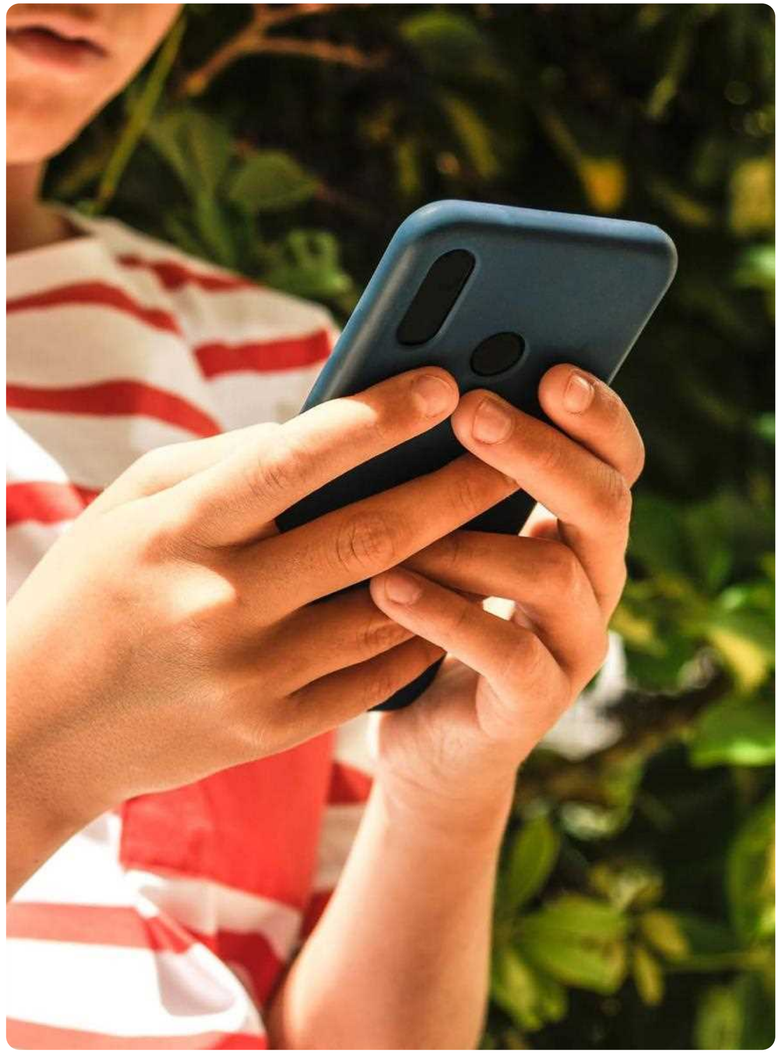
However, even in environments which parents broadly deem as safe for children – like gaming platforms – they acknowledge there are still risks. For example, many parents in focus groups discussed how the chat functions on gaming sites could expose children to harm – including contact from strangers and age-inappropriate content.

Figure 9. Parents view social media platforms as less safe than other online spaces:
Safety of online environments as perceived by parents



QOSAP4A. To what extent do you think the following online environments are safe or unsafe for your <age> year old <son/daughter>?
Base: 1,270 parents of children aged between 9-16





Children also believe safety varies across platforms. YouTube and WhatsApp were generally perceived as safer, due to age restrictions and safety controls, while TikTok and Snapchat are viewed as less safe due to higher rates of bullying and exposure to harmful content.

Boy, 13

"I know WhatsApp's quite safe because you have to properly enter their number, and if it's just a random person messaging you usually there's a really quick block button."

Girl, 13

"Some places, like Snapchat, I don't think that's good for anyone because you can just talk to strangers and perhaps see harmful stuff."

Girl, 11

"I don't think it is safe for young people - it's whatever TikTok brings to your feed that you watch."

Children report encountering more age-appropriate content online – yet harmful content persists

One reason why children may see the online world as getting safer is reduced exposure to age-inappropriate content. The majority (54%) of children report that content they have seen online recently is more child-friendly. This is especially true for those who say they are active online, with 74% saying the content they have seen recently is more child-friendly and safe.[7]

However, despite these positive perceptions, children are not free from negative content online. Our latest Children's Wellbeing in a Digital World report showed that while some individual harms have lessened, the overall level of harm experienced by children online has remained persistently high, with two-thirds (68%) of children experiencing harm online (for the third year in a row).[xiv]

7. *We define 'active' users as those who say they mainly post and comment 'a lot' on social media, while 'passive' users say they only really browse/scroll through and don't tend to post or comment on things.*

When we asked children about their experiences since the Children's Safety Codes came into force, 49% of children said they had experienced harm online in the past month.[8] Some of the most common harms experienced include seeing violent content (12%), content that promotes unrealistic body types (11%) and hateful content (including racial or homophobic content) (10%) – all of which should be prohibited under the Children's Safety Codes. An example that was discussed in focus groups was the unintentional exposure though social media feeds to the assassination of Charlie Kirk.

Alongside exposure to harmful content, families also spoke about other ongoing negative experiences children were having online, including approaches from strangers and bullying.

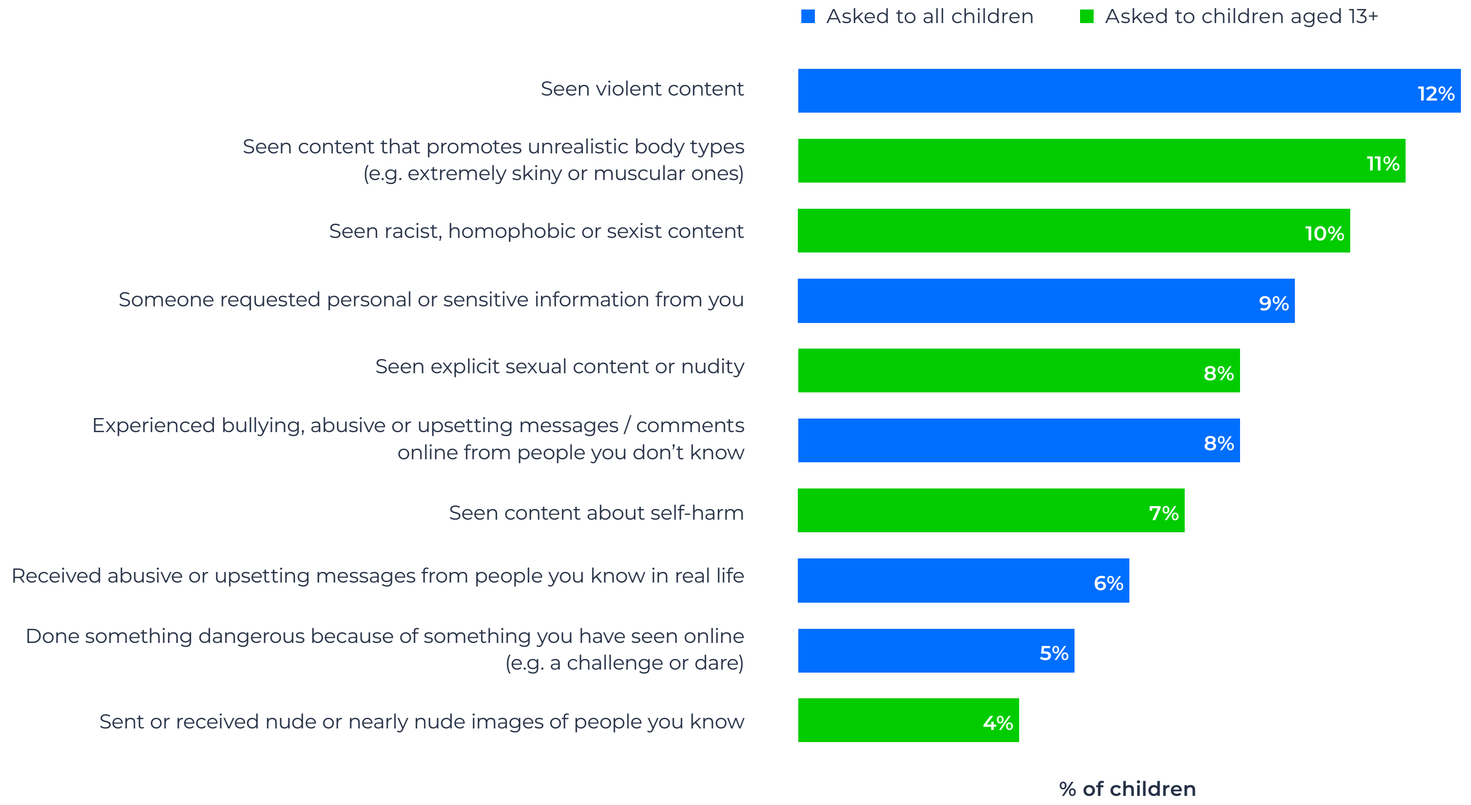
Girl, 14

"I saw it [video of Charlie Kirk assassination] on Snapchat. I broke down into tears and then told my mum immediately."

Dad of Girl, 11

"On WhatsApp and Snapchat, they have these group chats with kids from other schools my child won't even know, and they can say some horrible, nasty things."

Figure 10. Harmful content persists: Children's self-reported experiences of online harms in September – October 2025



Q51B. Have you had any of the following experiences online in the past month?
Base: 1,270 children aged 9-16

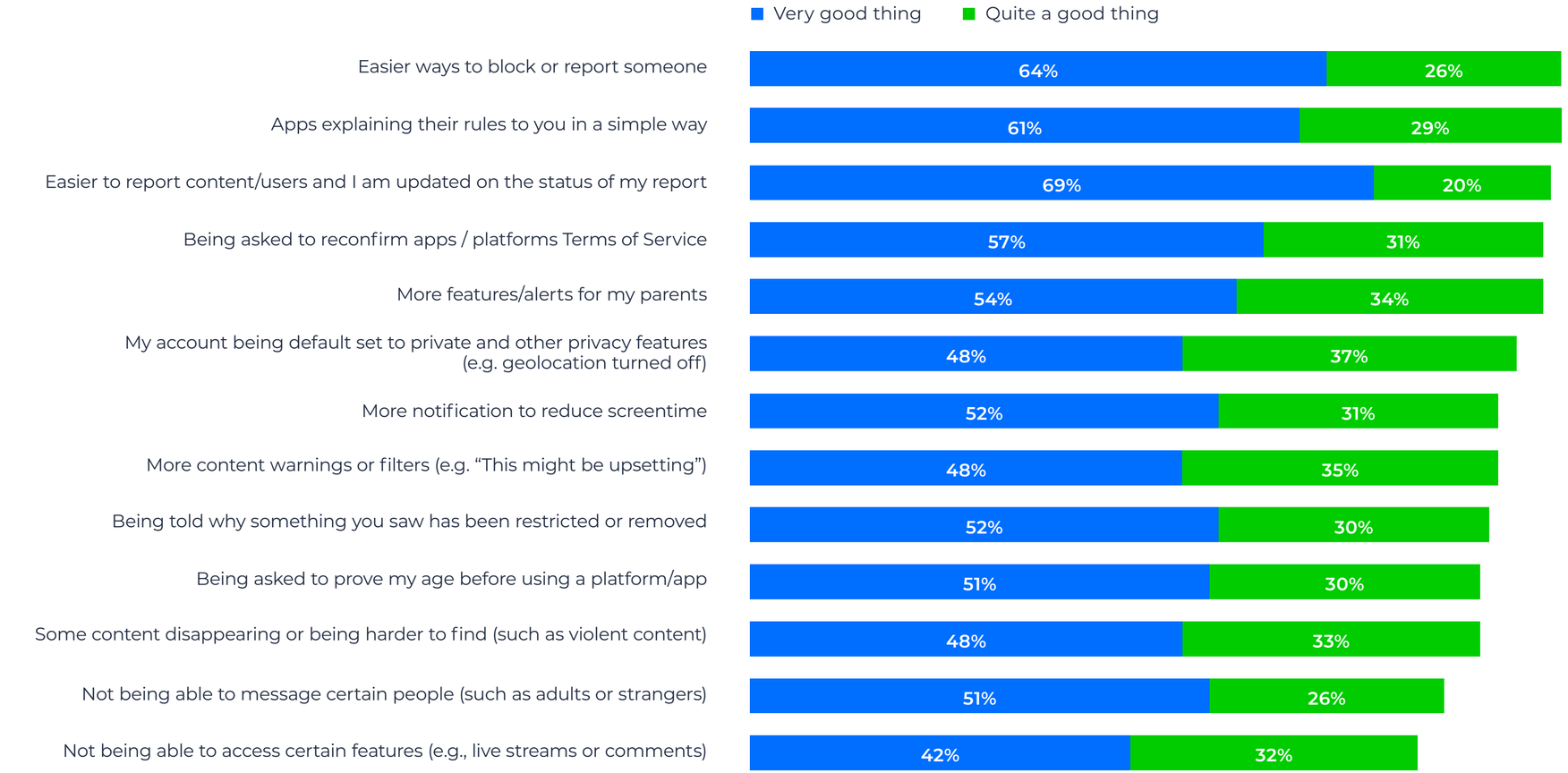
8. *Children were asked in September – October 2025 the follow question: Have you had any of the following experiences online in the past month?*

Children view new safety measures positively – but recognise these measures are not perfect

Overall, children were positive about the safety measures they had noticed being implemented online. Amongst children who have noticed them, changes related to blocking and reporting other content or users were most likely to be seen as positive, with 90% of children supportive of them. This is encouraging as previous research by Internet Matters found that reporting online harm was low due to complex processes and a lack of trust that platforms would act on reports.[xv]

All measures received strong support from children of all ages, including not being able to message certain people such as adults or strangers and not being able to access certain features (such as live streams or comments) – 77% and 74% of children respectively saw these changes as a good thing.

Figure 11. Changes to online spaces are viewed positively: Beneficial changes noticed by children



QOSAC4. Do you think these changes have been more of a good thing or more of a bad thing? Base: floating bases depending on whether child had noticed change

In focus groups, it was clear that children understood that these measures had been introduced to keep them safe online by preventing them from viewing harmful content and having harmful interactions.

However, there were some friction points for children. Children described finding safety measures annoying when it stopped them doing something like playing games with friends or accessing support networks – experiences children viewed as positive for their wellbeing.

There was also recognition amongst children and parents that the measures are not foolproof and cannot always be relied upon to protect children from harm, because they can find workarounds or because the measures are not consistently effective.

Boy, 15

"I think it's good so people who aren't the right age can't get onto stuff they are too young for."

Girl, 13

"[Private social media accounts] make it much more safe because random people can't just message you a lot of the time."

Girl, 11

"I think it's good because it keeps us from viewing adult content which is not going to be good for our mental health."

Girl, 16

"It's not practical because the more you restrict it, the more people are going to want to get past that age restriction"

Boy, 12

"Before you could talk to anybody, but they added age group limits so you can only talk to people in your age group. So if my friends are younger or older than me I wouldn't be able to talk to them."

Girl, 15

"There are websites that are support websites to help with things such as eating disorders and suicide, and they've all been censored".

Gaps in the Act: Excessive screentime and persuasive design

While the changes introduced under the OSA are broadly welcomed, they do not address what children and parents describe as their most immediate, day-to-day concern: the amount of time children spend online.

Children and parents described how children struggle to regulate their device use, spending large amounts of time online even when no longer enjoying it, or at the expense of activities like homework or family time.

These experiences align with findings from Internet Matters' 2026 *Children's Wellbeing in a Digital World report*, which shows not only are children spending more time online, but that this is having a negative impact on their wellbeing.[xvi] For example, 46% of children reported they keep playing the same games or watching the same TV shows or films even when not enjoying them, while 45% admit to stopping playing sport or doing exercise because they want to play video games, watch TV or be on social media. They are also choosing technology over sleep, with three in five (59%) children saying they stay up late on their devices.

Dad of girl, 11

"I don't think my children are particularly at risk from strangers or exploitation. I think it's more just wasting their time and rotting their brains looking at rubbish."

Girl, 12

"My screentime is like 8 hours a day and in that time I'm not doing anything else. I'm just eating, then going on my phone, then going on my iPad. I'm just on my phone and I'm forgetting about homework."

Girl, 16

"I definitely say I spend a lot of time on my phone. I'm on it at 3AM on a school night."

This behaviour does not occur in a vacuum. It reflects the commercial and design choices that shape children's online environments. Many platforms use features such as personalised algorithms, infinite scroll, autoplay, and streaks to capture and retain users' attention.[xvii] Children and parents recognise these dynamics, describing how algorithmic content delivery keeps them scrolling and can even expose them to unsuitable content.

Girl, 12

"With TikTok or YouTube shorts...it's just the endless cycle of scrolling. It never has a point where it stops."

Gaps in the Act: Addressing AI-generated content

Another concern raised by children and parents is the increasing amount of AI-generated content in their feeds. Children described encountering clearly "obvious" AI content, such as cartoon characters, alongside more realistic content, like celebrities or animals doing day-to-day activities, which was harder to identify as AI.

Girl, 14

"There's also a lot that you can't really tell what's an actual person and what's AI. It's quite funny, but it's kind of sad that you can just make anything. It's kind of creepy."

Concern about AI-generated content is echoed in previous research by Internet Matters, which found that 63% of children are worried about the growth of fake news and AI-generated content.[xviii] Over a quarter (27%) of children have seen a fake or AI generated news story and believed it. When asked how they felt about this, children and young people reported feeling confused (30%), annoyed (28%) and embarrassed (10%).

There was also worry around generative AI creating explicit images. While some had heard about this through the news, others had direct experience. One parent said that it was common amongst their children's age group to hide their faces in photos so their image could not be used to create such content. This concern is reflected in research exploring children's experiences of nude deepfakes, which found that 13% of children had encountered a nude deepfake and 55% were more concerned about a nude deepfake image being shared of them than a real nude image.[xix]

Girl, 16

"I feel like people can use it in really malicious ways. I had something happen to one of my friends where someone took her face and made her nude."

Interestingly, parents were less concerned about AI chatbots. As noted previously, these platforms were generally seen as safe by parents. While there was slight concern amongst some that prevalent use may limit children's learning and development – conversation of the risks posed were minimal. This may suggest that AI chatbots do not pose significant risks for families, but it is more likely that parents are unaware of the risks and of their children's use, particularly as they are integrated into platforms that children already use. In focus group discussions, parents did not initially recognise their children were using them until specific AI chatbot names were mentioned. Given research shows AI chatbots present a range of risks for children, from providing inaccurate and potentially harmful advice to impacting cognitive, emotional and social development, these risks cannot be managed by families alone.[xx] Instead, new and emerging technologies must be made safe for children prior to widespread use, not after.

Children and parents are optimistic that the online world is becoming safer, with many seeing positive safety measures implemented across children's accounts. However, this view is by no means universal. Exposure to harmful content remains prevalent and children continue to have harmful interactions online – two challenges the OSA was designed to address but is not yet delivering on. In addition, important risks remain outside its scope, including emerging harms like AI-generated content and the issue of most concern to parents and children: the amount of time spent online. If we are to measurably improve children's online lives, these gaps must be addressed through new legislation, alongside strengthening existing regulation.

Section 4:
Improving children's online safety: *what more can be done*

The OSA was heralded as a step change for children's online safety. Yet, for many families, it has not led to measurable change in children's online experiences, nor addressed the issue most salient to them: the amount of time children spend online. This has fuelled public debate around alternative approaches, including proposals to ban social media for under-16s.

While some parents are in favour of a ban - arguing it will improve children's wellbeing – many are concerned that a ban would be ineffective in practice or even detrimental given the social and developmental role online spaces play in a digital world. Alternative measures include stronger enforcement of existing laws, restricting certain platforms and functions, and more parental involvement in age verification.

Support for banning social media is strong but many see limitations

According to Internet Matters Pulse, a survey of 2,000 UK parents conducted in November 2025, 62% of parents support a ban on social media for under–16s, up from 44% in August 2024.[xxi] When discussing an Australia-style social media ban (where under-16s are prohibited from having accounts on certain social media platforms) – some thought this was the best way to protect children in a digital world.

Girl, 14

"I think the ban for under 16s is the best idea because it's just really difficult to stop yourself... I just want to scroll."

Mum of boy, 13

"Let kids be kids without social media. Let them go out and play and enjoy themselves."

Dad of girl, 11

"A blanket ban on social media is going to be a lot more effective than the sorts of things they're trying to do at the moment."

However, this view was by no means ubiquitous, with some believing the cost for children would be too high – preventing young people from doing things that are beneficial to them like communicating with friends or accessing support networks.

Others believed that a blanket ban on social media would undermine the nuance of online spaces. It was felt that different platforms were suitable for different ages, and that a 15-year-old should be allowed to do and see more online than an 11-year-old, for example. As a result, there was support for a more nuanced approach where restrictions were based on the risk posed by each individual platform and its features.

Mum of girl, 11

"What about all the good things we've talked about, learning and creativity, that would be taken away?"

Boy, 13

"[Social media is] how we talk outside of school. So I think if that gets banned, this is not really good."

Parents were also concerned about the unintended consequences of a ban. They felt that social media was too ingrained in children's lives to easily be removed and that the demand would create a "black market", meaning children would access harder-to-regulate platforms and be even more susceptible to online harms.

Dad of boy, 12

"There'll probably be a black or grey economy that emerges, where people can buy devices set at different ages. That's the danger of driving things underground and unregulated markets."

Mum of girl, 11

"Taking away things just creates a black market and a vacuum for something else much, much darker, much harder to regulate."

Girl, 11

"You could probably have different age ranges on apps. So, for example, on TikTok, maybe as you're signing in it could be you have to select an age range for you so then it will personalise the settings."

Regardless of whether people supported a ban or not, there was scepticism that it would work in practice. One challenge raised was that VPNs could be used as work arounds. This scepticism from both parents and children may reflect the weaknesses of current safety measures, especially age checks, resulting in a lack of confidence that effective solutions exist.

Dad of boy, 15

"I think it's [the ban] a great idea in theory and I applaud its intentions, but I don't see how that's feasible, because kids will always find a way."

Boy, 12

"I think what will probably happen is some people use like VPNs to change their location on their devices to be somewhere without a ban."

Alternatives to a blanket ban on social media

Alternative measures to banning social media for under-16s which parents and children discussed, included stronger enforcement of existing legislation, stricter age-checks (including more parental involvement) and restricting specific harmful features.

To make age verification more difficult to bypass, parents were open to the use of a range of methods including more parental involvement. Suggestions from parents included multiple step-processes, the use of unique identifiers such as a National Insurance Number and parents having to verify their age to register a child. Some also mentioned the idea of a centralised system where people could register and prove their age once and this would then apply across all social media platforms and websites.

Another suggestion was making social media a paid-for service, where signing up requires a parent to input their bank details. Not only would this ensure children can only access age-appropriate platforms, but parents felt this would allow them more control and knowledge over what their child is doing online. More oversight of what their children are doing online was important to parents.

Parents also suggested that children should be restricted from some platforms more than others. Several parents wanted social media the most tightly restricted because of the content and features available. This reflects the views of parents that social media platforms are less safe than other environments such as gaming or search services. Online gaming platforms with chat functions were also singled out by parents as needing tighter restrictions on who could use them.

Dad of girl, 14

"Maybe if they need to provide a National Insurance Number along with a parent Face ID or something...there needs to be a two-tier or three-tier process in order to get onto that platform."

Dad of boy, 15

"It would be nice if we all had to just register with one central base which says if you are going to any social media you need to register here."

Mum of boy, 12

"I think the aim is to make it better, but it's just not strict enough. If they make it more strict, then obviously it would be a lot harder for them to get around it."

Girl, 16

"I feel like sometimes when I report the accounts, nothing actually happens. I feel like they can make that a bit better where something actually happens."

Children and parents emphasised that simply restricting access to platforms is not enough; broader issues with platform design also need to be addressed, such as infinite scrolling and gamification features that encourage prolonged use. Many suggested targeted restrictions on specific features rather than banning entire platforms, for example limiting chats with strangers or disabling location sharing. Children also expressed a desire for more straightforward and effective ways to control what they see online, so that content preferences are reliably respected and violent or unwanted material is blocked.

There was broad agreement among both parents and children that the Government should have the power to regulate platform features – enforcing regulation through fines and penalties. This was seen as necessary, as there was little confidence that platforms would voluntarily alter features in ways that might reduce user engagement or profits.

Banning social media for under-16s has received significant political and media attention.[xxii] For some parents, this approach is appealing as a way to prevent harm and improve children's wellbeing, while also reducing the burden on families to constantly manage and navigate different settings, apps and decisions about their child's online lives. For others, the cost to children would be too high, given the social and developmental role online spaces play in a digital world. Regardless, parents on both sides of the debate are concerned that a ban would be ineffective in practice. As alternatives, parents and children support stronger regulation, including more tools to facilitate easier parental oversight, more effective age checks, and restriction and limitations on the most risky platforms and features.

Dad of girl, 14

"[Algorithms] are definitely a worry for social media. It can really take you down a rabbit hole."

Mum of girl, 13

"I would love Snapchat to be banned first of all, so I can just, cut a break from the constant harassment."

Non-binary child, 13

"The solution I would pose is removing public chats and making them private so you won't join a group with somebody you don't already know."

Dad of girl, 15

"Something that's catered to kids like Roblox, there are adults accessing it."

Girl, 13

"[If I could make one change to social media] I think taking away seeing locations is a good thing, as well as making limited screen time a thing."

Dad of boy, 15

"I think it's definitely the platform's responsibility."

Girl, 12

"Snapchat probably won't get rid of streaks because I feel like people would stop using it, and then Snapchat's net worth and income wouldn't be as much as it is."

Mum of girl, 11

"We can't assume that the onus is on the platform to do the educating, because it's not going to: it wants you to be on there. It's their own financial gain for you to be on their platform, because the longer you're on it, the more they're making in sales and sponsorship."

Girl, 12

"I think you should select things you want to watch, and it will block any other things. Violent content or anything like that, it would block it so you couldn't see it, so it would be more safe."

Girl, 13

"I don't think that there needs to be like a full ban. I think that there should just be like time limit on apps so people aren't spending as much time."

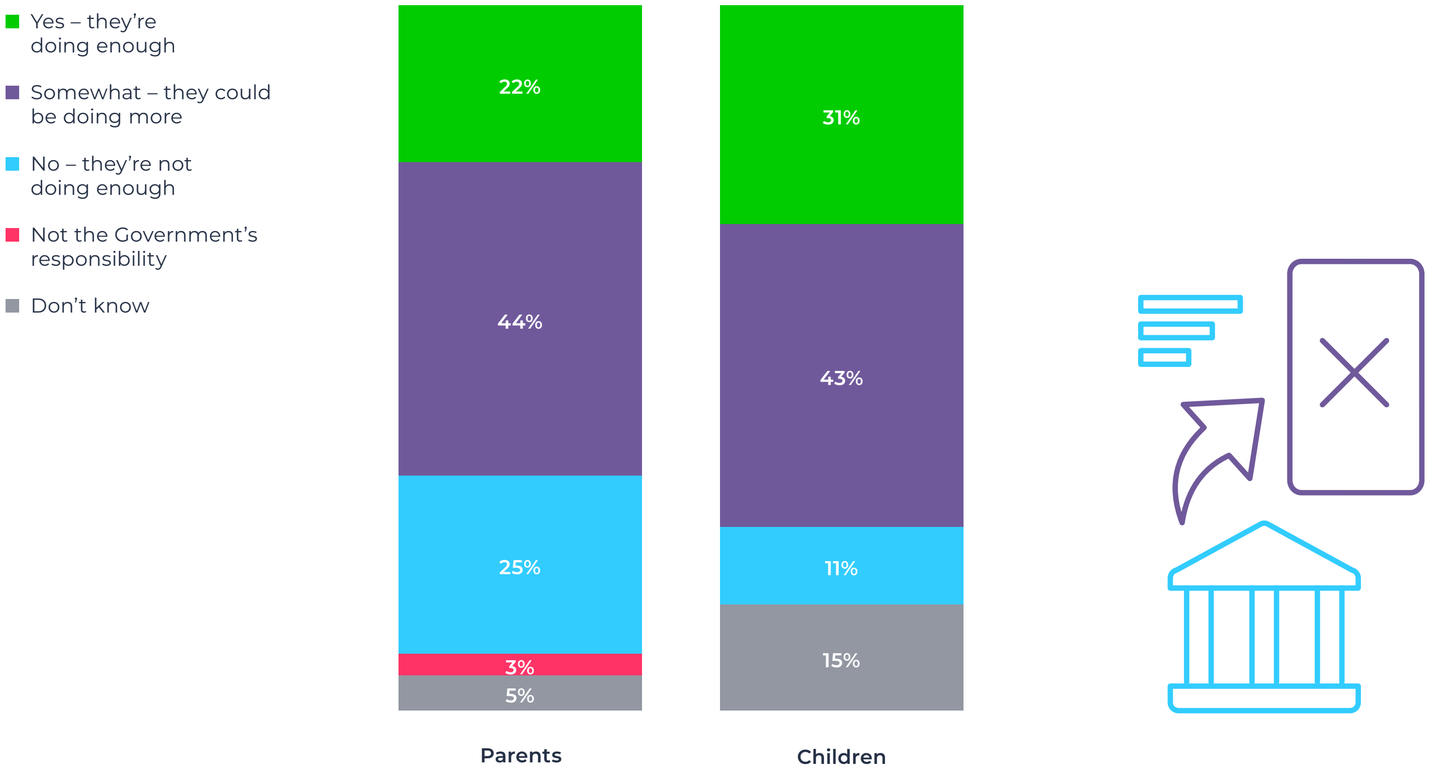
Section 5: Ownership of online safety: *a shared responsibility*

Parents see themselves as ultimately responsible for their child's online safety but recognise they cannot do it alone. They also see a role for government and platforms, believing they can and should do more. Children similarly view their online safety as a shared responsibility with parents, schools, government and platforms all having a role to play.

Parents and children want the Government to do more

Government regulation of online platforms is widely acknowledged as necessary to keep children safe online, with parents and children alike believing the Government and platforms should be doing more. Only 22% of parents believe the Government is doing enough to protect children online, while 44% say they could be doing more. Similarly, fewer than a third (31%) of children believe the Government is doing enough, with 43% saying more could be done. This was reflected in focus group discussions where parents emphasised the need for platforms to do more and be held accountable by government.

Figure 12. Parents and children want the Government to do more: Whether people think enough is being done by the Government to protect children online



QOSAP4D. Do you think the Government is doing enough to keep children safe online? Base: Parents (1,270) of children aged between 9-16
QOSAC10. Do you think enough is being done to keep children safe online (e.g., by the Government, tech platforms, etc.)? Base: 1,270 children aged 9-16
n.b. We did not ask children whether they thought it was the Government's responsibility.

However, parents noted, likely based on their experience of existing measures, that regulation is only effective if it is well designed and enforced. Without this, it can fail to deliver meaningful change. As a result, parents supported a firmer government approach towards platforms, alongside effectively designed government policy.

Parents see themselves as responsible for children's online safety, but recognise their limits

Despite support for stronger regulation of platforms, and more effective enforcement, parents ultimately see responsibility for children's online safety as resting with them. This includes monitoring their children's online activity, setting boundaries and controls, and fostering open communication and trust. Parents view these as responsibilities that cannot be delegated to schools, platforms, or government.

How parents viewed their role changed with the age of their children: those with younger children focused more on the use of parental controls and monitoring, while those with older teenagers placed greater emphasis on trust and communication.

Parents also recognised the limits of what they can do. A difficulty that some parents faced is being less "tech-savvy" than their children, leaving them unsure how to effectively manage what their children access and see. For example, children may hide apps on their home screens or bypass parental controls. In these situations, parents felt that the responsibility should fall on the creators of the technology to ensure children's safety. Parents also described difficulty keeping up with the different tools available to help manage their children's online experience.

Parents were also aware of the limits of their control. They recognised that different families have different rules and that they do not always have a full view of, or control over, what their child is doing online, especially when at the home of other parents, relatives or their child's friends. Moreover, even if their own child acts responsibly online, the behaviour of others could still affect them.

Mum of girl, 11

"The platforms can 100% see what is bad content. They 100% can see that and it's just whether they choose to remove it or not."

Mum of non-binary child, 13

"It's got to be down to the platform, hasn't it? The platforms need to be more stringent... each platform really has to take responsibility and put the work in themselves."

Mum of girl, 11

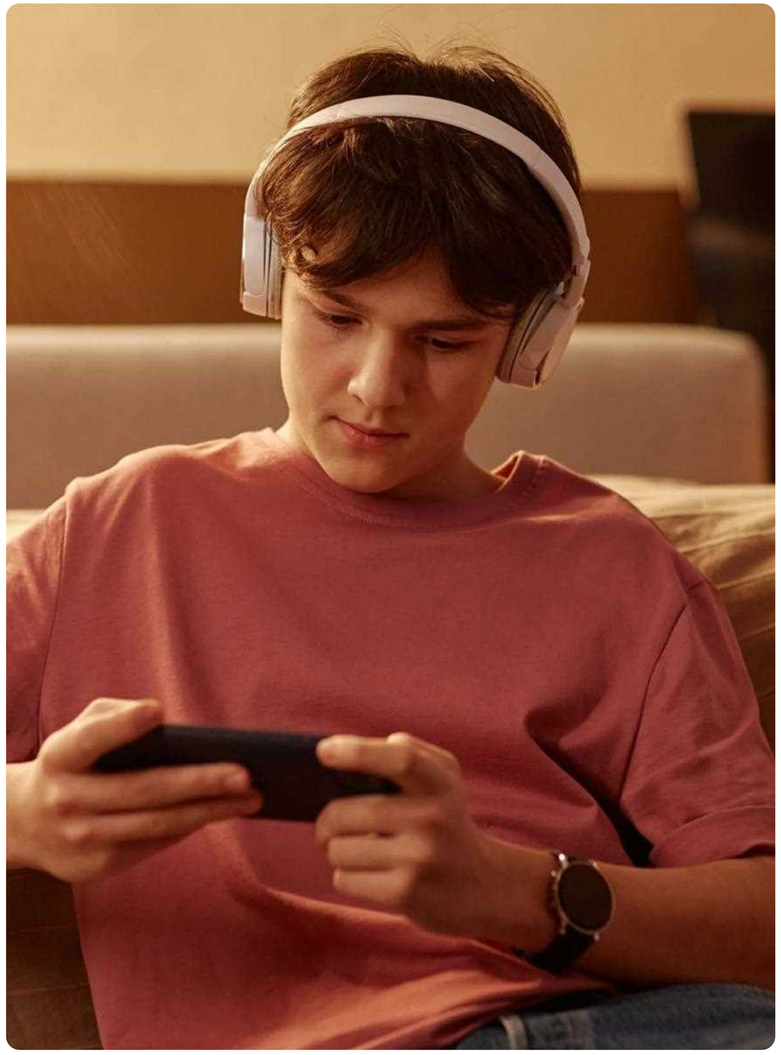
"I think ultimately, as a parent, the bottom line is you. Because if at some point if something fails and your children suffer as a result, it's not the Government or Big Tech or any of these companies that are going to feel the effect. It's you and your child."

Non-binary child, 13

"I believe the parent should be responsible for keeping an eye on their kids' online activity."

Dad of girl, 11

"I think generally when government regulations come in, they tend to be so clumsy and never effective enough."



Dad of girl, 14

"What you'll find now is that the kids know more than we know in terms of how to disable them. We've got the parental controls on, but they probably unlock them."

Mum of boy, 13

"I've never looked at parental controls... I'm rubbish with technology. I wouldn't know how to operate a parental control... so I just rely on good old-fashioned trust."

Mum of non-binary child, 13

"We do what we can, but our kids are all clever and savvy and they can get around stuff."

Dad of girl, 11

"My daughter, can't install any app without my consent, without my password."

Mum of girl, 12

"I can put all the checks and measures in, and I can be keeping an eye open on what she's watching, listening to, who she's chatting to [...] And then she could go to a house down the road and visit somebody whose parents don't care, and they've got zero checks and measures."

Dad of boy, 15

"It's about trying to maintain an open level of communication with your children and take an interest in their interests."

Dad of girl, 11

"It's an ongoing battle. Her mum doesn't believe her phone is a problem, and as we are a blended family, we don't have total control if she goes to her mum's."

Resources and guidance are valued by parents

Parents expressed that more guidance from both governments and platforms would be helpful to support them. They wanted more information on popular trends and influencers on social media, detailed guidance on how to use parental controls, and campaigns to raise awareness of potential online risks.

Parents also saw a role for schools, with some seeing the role of school as working well, while others thought they could play a more active role in supporting children and families.

Mum of girl, 16

"I just wonder if, if some of us were more aware of the stories then maybe that might make people think 'what's my daughter up to in her room?'."

Mum of boy, 16

"If they could do a little course for parents and explain - if your child's on TikTok, this is how you set up controls, if they're on different platforms, tell them what the dangers are."

Children cannot navigate online safety on their own

Children see parents as central to their online safety. This includes educating them on how to stay safe online, explaining potential harms, and managing their access to online spaces when necessary. Alongside parents, children see school as an important place for learning about online safety and setting boundaries, such as around phone use. However, they view the role of schools as less significant than that of parents.

Children also recognise that they can take steps to protect themselves and improve their wellbeing, such as by managing how much time they spend online, controlling what information they share, and choosing which platforms they use. This sense of responsibility grows as children get older. However, children recognised how difficult this can be, given the persuasive design of many platforms.

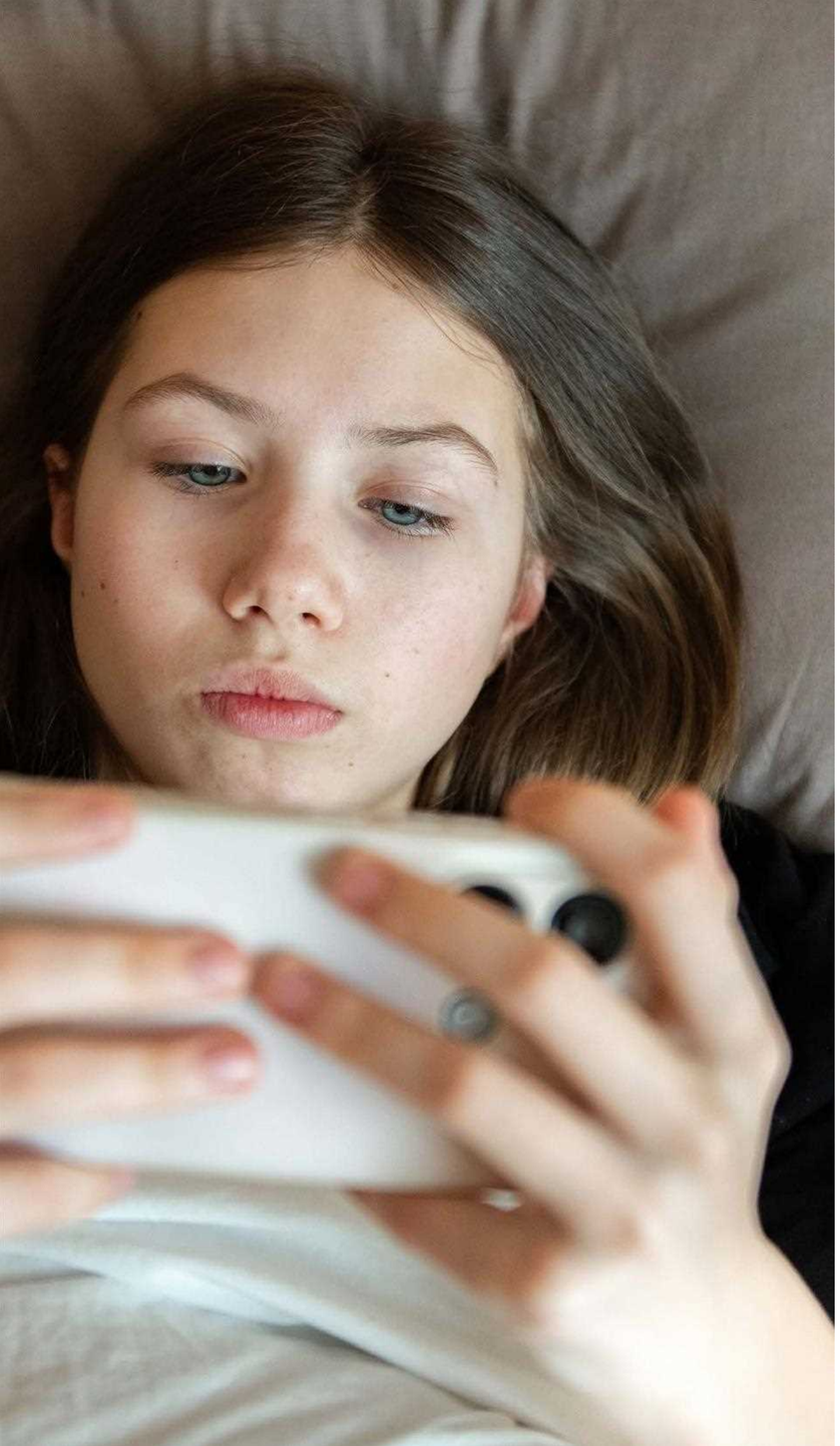
Boy, 15

"I think it's your own responsibility to stay safe online, like by setting your accounts to private."

Non-binary child, 13

"The company wants you to spend as much time on its app or game as possible, so it makes it addictive."

Government regulation and platform responsibility is seen as necessary by both parents and children to keep children safe online, but this alone is not sufficient. Ultimately, parents remain central to children's online safety, and must be supported by government, platforms, and schools to help their children thrive in a digital world.



Conclusions and recommendations

This report provides an early view of the impact of the Act on children's online safety. While many of the protections relating to children have been in force for a short time, families are seeing some positive changes. This includes more child-friendly content, limitations on risky functions like location sharing, and greater control over children's online experiences. These changes are broadly welcomed and suggest the OSA is beginning to shape children's online environments for the better.

However, despite this progress more can be done. Children continue to encounter harmful content at unacceptable rates, while age verification measures are often ineffective in practice or easy to bypass. Furthermore, many of the issues most important to families, such as managing the amount of time children spend online, and the risks from AI, are not well addressed by the Act. As a result, responsibility for managing children's online safety continues to fall heavily on families.

With growing focus on improving children's online wellbeing, and as government considers further steps to protect children in a digital world, this is an opportunity to drive better outcomes for families. To do this, safety measures need to be effective in practice, designed around the needs of families and focused on creating positive online experiences for children. Only then will we deliver meaningful change for children's online safety and wellbeing.

Across all online services used by children – including social media platforms, gaming environments and AI chatbots – initiatives to improve children's safety and wellbeing must be based on the following principles.

Safety-by-design

Services must be built on the principles of safety-by-design, **meaning children's needs are considering and addressed from the outset, not after harm has occurred.** Where platforms are to be accessed by children, then their safety should be prioritised over profit and for services not appropriate for child users, safeguards, such as highly effective age assurance, must be put in place before they are brought to market. Safety-by-design should also be considered before new features and functionalities are added to existing platforms.

Risk based approach to children's access

Children's access to online spaces should be determined by the level of risk a platform or service presents, and the effectiveness of the safeguards it provides, rather than through blanket bans on categories of platforms. A risk-based approach ensures children can access digital services safely, while preserving opportunities for age-appropriate engagement and learning.

When assessing risk, the following factors should be considered:

- **Addictive design features** including personalised algorithms, infinite scroll, and engagement streaks.
- **Functionalities that present potential harm,** such as location sharing, in-app spending, chat functions and disappearing content.
- **Emerging risks from AI** including mimic features, deceptive or flattering language and realistic AI content.
- **Supportive safeguards** such as positive nudges, content filters, and enhanced reporting and redress systems.
- **Parental controls** including mechanisms for parental consent and oversight.

Age-appropriate experiences

Alongside a risk-based approach, **children's access to content, features and functions should be tailored to their stage of development, rather than a one-size-fits-all approach.** Experiences should reflect children's evolving capacities - their heightened vulnerability when younger and their growing autonomy as they grow. Access should therefore be graduated over time, recognising that a 7-year-old and a 17-year-old have very different capabilities, for example.

Age assurance

Fundamental to delivering the above is online platforms and services' ability to reliably determine the age of users. **Highly effective age assurance should be used to accurately establish users' ages,** allowing services to tailor age-appropriate experiences and to enforce age requirements, ensuring children cannot access platforms not designed for them.

Media literacy

Parents and children both play a central role in keeping children safe online. To support parents in this role, **we must provide them with timely, engaging and trustworthy information.** This includes guidance on how to set up parental controls, through to clear, accessible explanations of how algorithms work and influence what children see online. **This should be delivered through a range of channels including platforms, government and trusted, specialist organisations, like Internet Matters.** Government should also use nationwide campaigns to reach parents and set expectations.

Equally important is teaching children the media literacy skills and knowledge they need to thrive in a digital world. Alongside parents, schools provide an excellent opportunity to deliver media literacy at scale, and we must ensure **the curriculum meets children's needs, including through clear guidance for schools, and training and resources for teachers.**

Media literacy can be defined as: being able to evaluate information and distinguish between what is true and false online; being able to create and share digital content responsibly and safely; and the awareness and ability to protect yourself from the risks of being online.

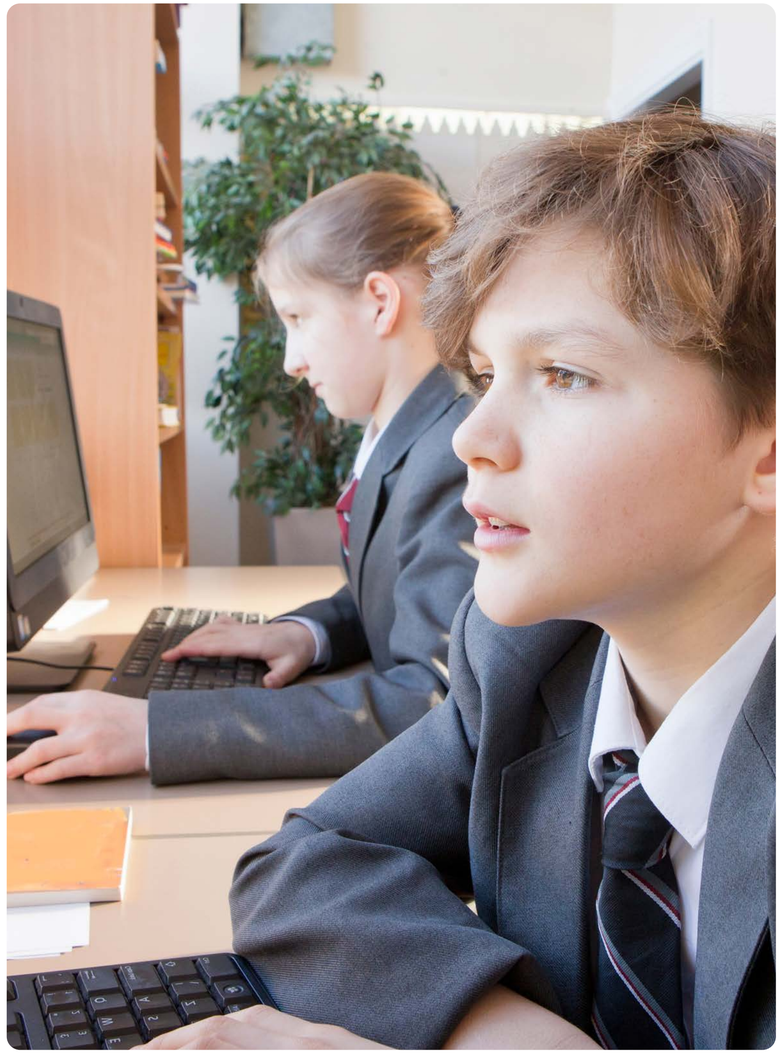
Platforms are also critical for media literacy and **should provide parents with easy-to-use parental controls, clear guidance, and accessible information.** Platforms should **embed media literacy-by-design, by incorporating features that actively help children to evaluate, question and contextualise the information they see.** This could include clear labelling of AI-generated or manipulated content, content warnings or prompts highlighting the source of information.

Enforcement, accountability and leadership

Regulation of online services will only be effective if it is backed by robust enforcement and accountability. **Government must ensure existing legislation is properly enforced and hold both regulators and platforms to account where it is not. It must also address gaps in the law without delay** – we cannot wait for harm to occur. Regulation should also enable swift action against services that breach the law.

Alongside enforcing regulation and holding platforms to account where they are failing to meet the needs of their users, government should also provide a blueprint for what good looks like when it comes to children's online safety. This should be developed in partnership with civil society, academic experts, platforms, and, importantly, children and parents.

Taken together, implementing these principles will improve children's online safety and allow them to thrive in a digital world.



References

i. Internet Matters, *Internet Matters Pulse.* https://www.internetmatters.org/pulse/

ii. Internet Matters, *Digital Wellbeing research programme.* https://www.internetmatters.org/digital-wellbeing-research-programme/

iii. Internet Matters (2026) *Children's Wellbeing in a Digital World Year 5.* https://www.internetmatters.org/hub/research/childrens-wellbeing-in-a-digital-world-index-report-2026/

iv. UK Government (26 October 2023) "UK children and adults to be safer online as world-leading bill becomes law". https://www.gov.uk/government/news/uk-children-and-adults-to-be-safer-online-as-world-leading-bill-becomes-law

v. UK Government (15 February 2026) "PM: 'No platform gets a free pass': Government takes action to keep children safe online". https://www.gov.uk/government/news/pm-no-platform-gets-a-free-pass-government-takes-action-to-keep-children-safe-online

vi. Ofcom (24 March 2026) "Statement: Protecting people from illegal harms online". https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/statement-protecting-people-from-illegal-harms-online

vii. Ofcom (1 April 2026) "Protection of children's duties under the Online Safety Act". https://www.ofcom.org.uk/online-safety/protecting-children/protection-of-children-duties-under-the-online-safety-act

viii. Ofcom (19 March 2026) "4chan fined £450,000 for not protecting children from online pornography". https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/4chan-fined-450000-for-not-protecting-children-from-online-pornography

ix. Ofcom (2025) *Children and parents: media use and attitudes report 2025.* https://www.ofcom.org.uk/media-use-and-attitudes/media-habits-children/children-and-parents-media-use-and-attitudes-report-2025

x. Internet Matters (11 April 2025) "Age assurance and online safety: What parents and children have to say". https://www.internetmatters.org/hub/research/age-assurance-online-safety-parents-children-opinions/

xi. 7NEWS (15 March 2026) "Underage Roblox accounts sold online allow predators to bypass safety measures protecting young gamers". https://7news.com.au/news/underage-roblox-accounts-sold-online-allow-predators-to-bypass-safety-measures-protecting-young-gamers-c-21525331

xii. Department for Science, Innovation and Technology (2 March 2026) "Growing up in the online world: a national consultation". https://www.gov.uk/government/consultations/growing-up-in-the-online-world-a-national-consultation

xiii. Internet Matters (4 December 2025) "New data shows no rise in children's VPN use after the introduction of online age checks". https://www.internetmatters.org/hub/research/data-shows-no-rise-childrens-vpn-use-amid-online-age-checks/

xiv. Internet Matters (2026) *Children's Wellbeing in a Digital World Year 5.* https://www.internetmatters.org/hub/research/childrens-wellbeing-in-a-digital-world-index-report-2026/

xv. Internet Matters (2025) *Understanding & improving how children report online harm.* https://www.internetmatters.org/hub/research/understanding-and-improving-how-children-report-online-harm/

xvi. Internet Matters (2026) *Children's Wellbeing in a Digital World Year 5.* https://www.internetmatters.org/hub/research/childrens-wellbeing-in-a-digital-world-index-report-2026/

xvii. 5 rights (2023) *Disrupted Childhood: The cost of persuasive design.* https://5rightsfoundation.com/resource/updated-report-disrupted-childhood-the-cost-of-persuasive-design/

xviii. Internet Matters (2025) *Informed or Overwhelmed? Understanding the impact of online news on children and young people's wellbeing.* https://www.internetmatters.org/hub/research/impact-online-news-childrens-wellbeing/

xix. Internet Matters (2024) *The New Face of Digital Abuse: Children's experiences of nude deepfakes.* https://www.internetmatters.org/wp-content/uploads/2024/11/Childrens-experiences-of-nude-depfakes-research.pdf

xx. Internet Matters (2025) *Me, Myself & AI: Understanding and safeguarding children's use of AI chatbots.* https://www.internetmatters.org/hub/research/me-myself-and-ai-chatbot-research/

xxi. Internet Matters (9 December 2025) "Australia's social media ban and why the UK might be next". https://www.internetmatters.org/hub/research/australias-social-media-ban-and-why-uk-might-be-next/

xxii. The Guardian (15 April 2026) "MPs vote against social media ban for under-16s a second time". https://www.theguardian.com/uk-news/2026/apr/15/mps-vote-against-social-media-ban-for-under-16s-a-second-time

About BMG

BMG Research specialise in delivering impactful insights to inform decision-making, shape policies and guide investments. Primarily based in the UK, they work closely with their clients to help them navigate complex challenges, set strategic priorities and assess the effectiveness of change. They leverage extensive subject knowledge and methodological expertise, combining these with cutting-edge analytics to create tailored solutions for each of their clients.

internet matters.org

Faraday Buildings,
Ground Floor,
1 Knightrider Street,
London, EC4V 5BT

info@internetmatters.org

InternetMatters

@InternetMatters

Internet Matters Ltd

@internetmattersorg