



**CYBERSAFE
KIDS**



The Year Little Changed

*More Regulation, More AI,
Same Old Problems*

Children's Digital Lives in Ireland, 2025–26

Deloitte.



The Year Little Changed

More Regulation, More AI, Same Old Problems

Children's Digital Lives in Ireland, 2025–26

The Year Little Changed

Welcome to *The Year Little Changed*, CyberSafeKids' tenth annual report, marking a decade of monitoring and highlighting how children in Ireland¹ experience the online world, and the ways in which policy and industry have (or more often haven't) kept pace.

This year's findings draw on our regular survey of thousands of children aged 8–15 across Ireland, focus group discussions with young people, and collaborative research carried out by students from Atlantic Technological University and University College Dublin, in consultation with academic supervisors and CyberSafeKids. Their work has added rich, independent insights into what children are actually exposed to in the online environments they use most.

As always, youth voice remains at the forefront of our findings, and the quotes you will encounter throughout the following pages shine a light on the realities of digital childhood today. Within this report, we examine what has genuinely changed in underage users' access to digital platforms, one year on from Ireland's Online Safety Code coming into effect and the publication of the EU Digital Services Act's Article 28 Guidelines. As you may have already guessed from the title of the report, little has changed.

Given the theoretically stronger regulatory landscape now in place across Europe, we take a close look at whether current child safety measures on popular platforms are translating into meaningfully better experiences for children. Unfortunately, progress here is also disappointing.

This year our spotlight falls firmly on Roblox, the most popular online environment for under-13s in Ireland. Roblox's lighter regulatory footing highlights a gap: regulation of digital spaces has simply not kept pace with where younger children actually spend their time online.

The report also tracks the exponential growth in children's engagement with generative AI – a theme we first raised in last year's findings. We simply cannot afford to be as slow off the mark in regulating AI as we have been with social media, particularly given how inadequate existing regulation is already proving to be in improving outcomes for children.

When it comes to the challenges of digital parenting, we look at the impact of the national collective 'hold off' movement, and the clear evidence that it is not reaching every community equally. Responsibility for children's digital safety must not fall on parents alone if protection is to be universally felt.

The report concludes with our recommendations, which centre on the need to think radically about how we address a problem fundamentally rooted in a business model that harms users and remains subject to far less scrutiny than any other industry. As always, our aim with this report is to raise awareness, but more than that, we want to build cohesion around a clear and shared set of societal solutions.

Finally, we would like to warmly thank Deloitte for coming onboard as our title sponsor for this year's report, and we hope that you will enjoy these ever-fascinating insights into digital childhood in Ireland: as you will see, there is clearly much more work to be done.



Alex Cooney
CEO & Co-Founder,
CyberSafeKids

In Their Own Words¹

I've been sent death/self harming threats saying I will hurt myself if you don't do this or I will kill myself if you don't do this or people telling me to kill myself or them telling me to cut deeper or for me to self harm when I already struggle with it. (12)

I saw someone in a game doing fake sex. (9)

Someone once slipped into my DM's and texted me saying that they would find me and touch me. (10)

So you know in yt so basically there are bots and they have disgusting profiles and they use fake likes to be the top comment. (11)

I seen someone getting stabbed. (11)

I was told that the person raped my parents in the basement whatever that means. (10)

Bot accounts were showing fake AI nudity. (12)

A guy friended me on Snapchat and I friended him back so he was like wanna be my gf I was gonna say no but I asked him how old he was he said he was 18 so I said I was 13 and he was like oh that's fine what's ur chest size. (11)

People send inappropriate stickers and pictures into a group chat. (13)

They said I'm a paddy and I probably need to kill myself. (12)

I have often seen nudity on Roblox such as inappropriate avatars and moaning in games with voice chat. (11)

A guy asked me to send nudes. (11)

I saw a man getting slaughtered and chopped off his testicle while he was upside down. (11)

Somebody said u are ugly and fat, they called me a loser and a nasty. (10)

My friends account got hacked and they were blackmailing her. (10)

Someone called me a bad word and I blocked but my friend had him added and he said he would smash my face in a door and said he would break all of my fingers. (10)

¹ 'Children in Ireland' and 'Irish children' are terms used interchangeably throughout to indicate *all* children living in Ireland, regardless of nationality.

¹ Below are a series of anonymous quotes from children that demonstrate exactly what they encounter every day online. The number in brackets indicates the age of the child.

Welcome from Deloitte



Nicola Flannery

Partner,
Digital Trust & Privacy

Trust is the foundation of every digital relationship, and children deserve the same protections we demand for ourselves. This year's CyberSafeKids report reveals both a challenge and an opportunity: digital environments are evolving faster than our collective ability to safeguard them. That's not a failure of technology, it's a call for better design.

CyberSafeKids' findings are unsparing, and they should be. Regulation has not kept pace with where children actually spend their time online, and too many platforms are still building in safety measures after the fact, rather than from the ground up. At Deloitte, we work across the ecosystem, with platforms, regulators, and policymakers, and we see the gap clearly.

The question now is whether we have the collective will to close it. That means platforms embedding safety by design, regulators moving faster and more decisively, and society demanding better of both. We're proud to support CyberSafeKids because this report holds up a mirror to the digital world children inhabit, and it refuses to accept incremental change. Neither should we.



Adrienne Daly

Head of Social Impact

Deloitte are proud to sponsor *The Year Little Changed*, CyberSafeKids' 2026 report. Digital trust and safety are frontline issues for society and for business. As a firm that helps organisations harness technology and data to grow, we also have a responsibility to ensure that this progress does not come at the expense of the most vulnerable but shapes a better future for individuals, communities and society.

Contents

About Our Research	08
By The Numbers	09
Age Not Assured	11
When Safeguards Fail	15
Growing Up On <i>Roblox</i>	37
Fool Us Twice	47
United And Divided	55
Our Recommendations	63

About Our Research

Quantitative research data was collected during the 2025–2026 academic year (September–June) via an anonymous online survey, conducted in 74 schools in Ireland, resulting in a total of 7,378 responses.

58 primary schools and 16 post-primary schools, representing 11 counties across Leinster, Munster, and Connaught took part. Over 6,000 of these responses are from 8–12-year-olds in primary schools, and more than 1,300 responses are from 12–15-year-olds in post-primary schools.

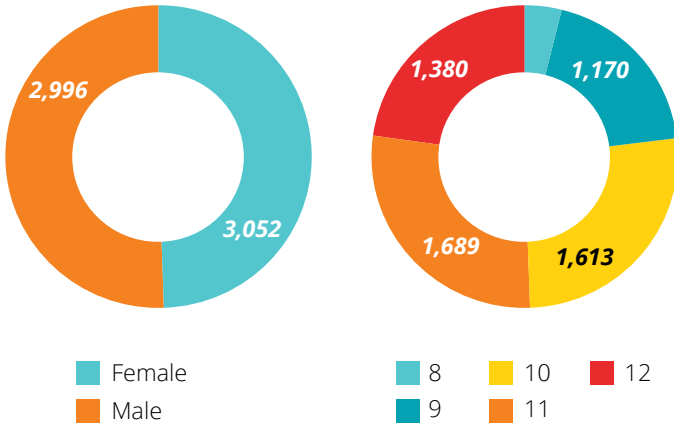
A diverse range of schools participated, including rural, urban and suburban schools, DEIS and non-DEIS schools, fee-paying and non-fee-paying schools, single-sex and co-educational schools, and Gaelscoileanna.

A breakdown of the dataset by gender and age is provided opposite¹.

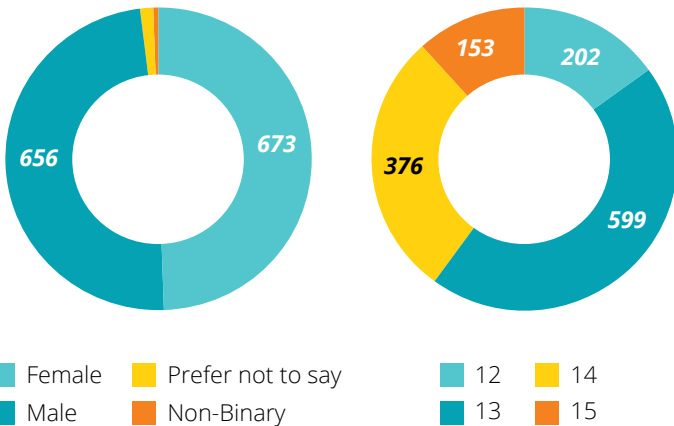
Numbers only tell us part of the story: children's voices tell us the rest. Throughout this report, we have quoted children to bring their views and experiences to the forefront. Qualitative testimonials and observations were gathered through the school surveys, while others were captured during focus group discussions with younger children (9–12) and older children (13–17).

Additionally, we have incorporated findings from three different research studies that were carried out in consultation with CyberSafeKids this academic year, by cyberpsychology students in Atlantic Technological University (ATU) and a computer science student in University College Dublin (UCD), both under academic supervision.

8–12-year-olds



12–15-year-olds



By The Numbers¹

8–12-YEAR-OLDS (Primary Schools)	12–15-YEAR-OLDS (Post-Primary Schools)	8–12-YEAR-OLDS (Primary Schools)	12–15-YEAR-OLDS (Post-Primary Schools)
📱 Own their own smart device 94% ↔ 63% tablet ↔ 57% games console ↔ 36% smartphone ↑ 30% smartwatch	99% ↔ 93% smartphone ↔ 57% games console ↔ 46% tablet ↔ 44% laptop	🔒 Play 18+ games ↔ 22% do 33% are boys, and 11% girls	↔ 32% do 51% are boys, and 16% girls
📱 Spend most of their time online ↑ Gaming 56% ↓ Watching videos 21% ↔ Messaging with friends 11%	↔ Messaging friends 33% ↓ Watching videos 31% ↑ Gaming 28%	👉 Have been bothered by something seen or experienced online ↔ 26% Most often occurs on ↔ Roblox 58% ↓ YouTube 34%	↔ 25% Most often occurs on ↑ Snapchat 48% ↓ TikTok 38%
🌟 Most popular digital environment ↑ Roblox 68% ↔ For messaging: WhatsApp 30%	↔ WhatsApp 85% ↑ For gaming: Roblox 67%	↔ Most commonly scams and fake information 36% ↑ and hate 33% ↔ ↔ 24% keep it to themselves 31% report it online	↔ Most commonly scams or fake information 41% ↑ and hate 38% ↓ ↓ 34% keep it to themselves 29% report it online
📺 Have accounts on regulated, 13+ social media apps ↔ 70% ↔ YouTube 63% ↔ Snapchat 21% ↔ TikTok 20% Non-account access 39%	↔ 99% ↔ YouTube 80% ↓ Snapchat 78% ↔ TikTok 72% ↔ Instagram 48%	🔥 Experience cyberbullying ↑ 28% ↔ Most commonly kept out of chat/ groups 15% ↔ receiving hurtful messages 10%	↔ 34% ↔ Most commonly kept out of chat/ groups 22% ↔ receiving hurtful messages 14%
📱 Use of AI ↑ 55% ↑ 59% look up information 47% ask fun or random questions ↑ 21% change/make images ↑ 16% chat and get advice	↑ 76% ↑ 75% look up information ↑ 35% ask fun or random questions ↑ 27% do school work ↑ 20% chat and get advice	⚠️ Encounter Sexual Content or Contact ↔ 15% of those 'bothered' report seeing or being asked for nudity or 'sexual things'	↔ 20% of those 'bothered' report seeing or being asked for nudity or sexual things ↑ 24% accessed sexual content this year: 27% of boys vs. 19% of girls

¹ All percentages have been rounded to the nearest whole number throughout this report.

¹ ↑ ↓ ↔ indicates whether figures are trending up, down, or largely unchanged compared to last year. Differences of up to 3–4% are marked as ↔ to account for normal variation in respondents' gender and age profile between the two years. Where no symbol is displayed, it was not tracked last year.

Age Not Assured

The *era of self-regulation* for Big Tech is over. We have heard this repeatedly in recent years from politicians and regulators both in Ireland and across Europe, but is it actually true?

I lied about my age. ⁽¹¹⁾

Despite new legal requirements designed to prevent this, 8–12-year-olds report still being able to sign up to, and actively use, platforms with a stated minimum age of 13¹ (referred to throughout as ‘13+ platforms’) without detection, suggesting that age assurance measures² are not functioning as intended on the platforms they use most.³

70% of 8–12-year-olds have accounts on one or more 13+ regulated platforms⁴. This figure is effectively unchanged⁵ from the 68% recorded before the regulatory deadline of 21st July 2025 – suggesting that neither the Digital Services Act nor Ireland's Online Safety Code is yet to have any measurable effect on underage access. Figure 1 shows the proportion of 8–12-year-olds with an account on each platform, comparing last year with this year (i.e. before and after the regulatory deadline of 21st July 2025). While there are some small differences by platform, these largely fall within the range attributable to sample variation, rather than a meaningful shift in underage access.

A Note on Regulation: YouTube, TikTok, Snapchat, Instagram, Pinterest, and Facebook are all subject to the EU's Digital Services Act (DSA), which requires platforms to take steps to prevent underage access.⁶ Most are also subject to Ireland's Online Safety Code (OSC), a separate set of obligations that applies to video-sharing platforms based in Ireland (this does not include Snapchat). Both sets of obligations were fully in force by 21st July 2025 – before this research was conducted. For brevity, we refer to these throughout as ‘regulated platforms’.

The EU Commission does not consider self-declaration to be an appropriate age assurance method to ensure a high level of privacy, safety, and security of minors in accordance with Article 28.⁷ Under the OSC, self-declaration of age alone is insufficient for age assurance where a service does not preclude ‘adult-only video content’, defined as pornography, or gross or gratuitous violence or acts of cruelty. The specific methods of age assurance to be applied are not defined but must be proportionate to the level of risk and comply with data protection principles.

¹ The digital age of consent in Ireland is actually higher by law at 16. 13 is the self-imposed ‘minimum age’ by most platforms.

² The term ‘age assurance’ is used throughout this report to indicate a mixture of methods such as age estimation and self-declaration to gain access to platforms or restricted features (and differs from age verification, which would require official documentation, e.g. passport or identity card).

³ A note on terms used: the words digital ‘services’ and ‘platforms’ reflect the language of both the OSC and DSA, and children are asked about ‘apps, games or services’ in the survey. There is, however, a growing legal movement to designate these digital services as ‘products’ to be subject to (and indeed prosecuted under) product safety or liability law, rather than treated as a category of ‘service’.

⁴ Of these, YouTube, TikTok, Instagram, Pinterest, Facebook are also subject to Ireland's Online Safety Code, which imposes additional, more specific age assurance obligations. Excluding Snapchat, which is regulated in the Netherlands,

⁵ This year is actually marginally higher than last (68% on same platforms in 2024–2025) but the difference falls within the range attributable to sample composition.

⁶ These are all designed as Very Large Online Platforms (VLOPs) and as such placed in the highest risk regulatory tier.

⁷ See footnote 56 in: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202505519

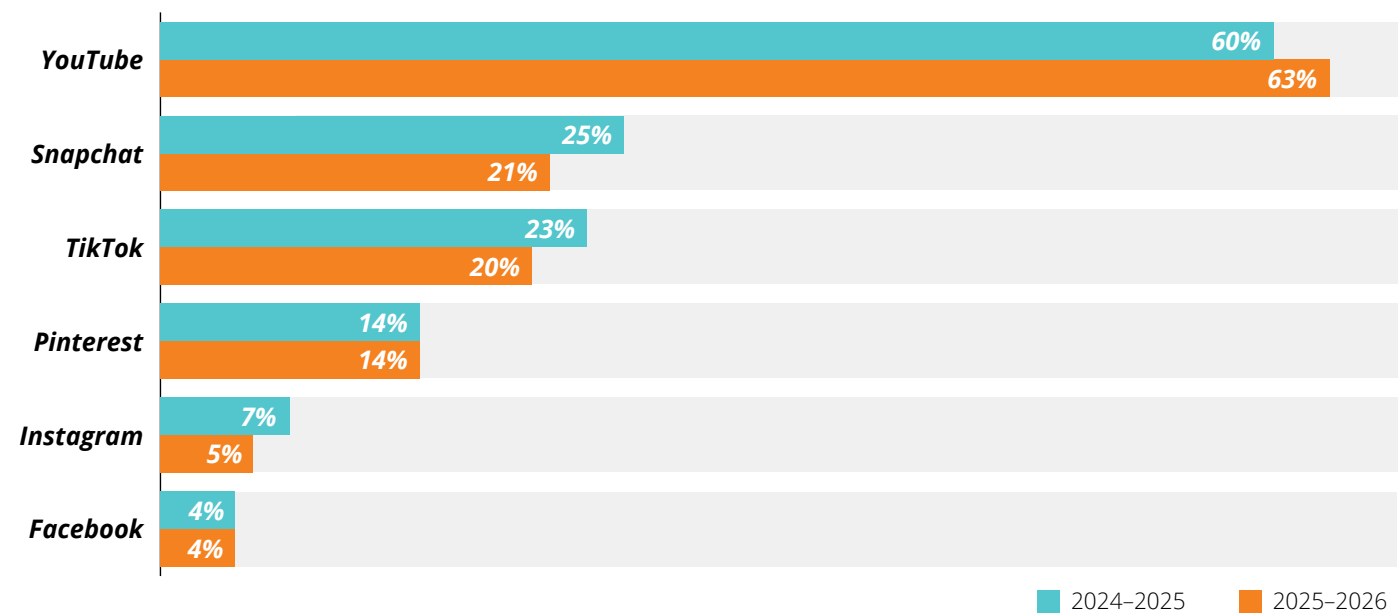


Figure 1: Own accounts on 13+ platforms (8-12-year-olds)

Getting In

This academic year, in a UCD undergraduate study⁸ undertaken in consultation with CyberSafeKids found that account creation still relies solely on self-declaration of age for YouTube, TikTok, Snapchat and Instagram. YouTube differs from TikTok, Snapchat, and Instagram in that it requires parental permission for a user who self declares an age of 13–15 years, in line with Ireland’s legal digital age of consent. There are no more additional age assurance measures, e.g. biometric face scans, payment card verification, applied at the account creation stage than there were before the regulatory deadline passed. Crucially, all of these platforms allow a child to avoid parental involvement and teen safeguards⁹ by self-declaring their age to be 16+.

Self-declared age clearly does not work as a barrier to access, and age-based safeguards – such as default privacy settings for teens¹⁰ – only work if a platform knows a user’s real age. In a focus group

conducted by CyberSafeKids this year, the 9–12-year-olds present indicated that they do not calculate a date of birth with care, but rather simply scroll back far enough in years to ensure they are not excluded on the basis of their age, thus potentially bypassing not just the 13+ minimum, but the age range which extra protections are designed to target. Without reliable age assurance on entry, such safeguards have nothing to act on.

Staying In

Regulated platforms are also expected to detect underage users, who state an older age at sign-up to gain access, using a mixture of methods such as behavioural or content analysis and user reports. Once detected, the accounts should be closed, or restricted accordingly.

Behavioural age assurance¹¹ may struggle to distinguish between adjacent ages, such as a 12-year-old and a 13-year-old, but the gap between our youngest research group (8 and 9-year-olds)

and a 13+ threshold is substantial – and detection rates remain poor even here. Isolating our youngest research group of 8 and 9-year-olds, we found that 62% have accounts on regulated, 13+ platforms.¹²

Only 27% of 8–12-year-olds say they have been prohibited from using their account(s) on games and apps they use (Figure 2). Importantly, when they are stopped, banned or blocked from accessing their accounts, it is seldom related to their age (Figure 3) and mostly occurs in gaming environments rather than on the 13+ regulated platforms. Children describe being suspended or banned from games due to poor behaviour (detected through moderation) or in response to a user report – a mechanism that can itself be misused, e.g. to exclude or bully another player. This is further supported by the fact that gaming is more popular among boys in our sample, and boys were also more likely than girls to report being shut out of an account (32% boys vs. 23% girls).

I got banned from someone false reporting me. ⁽¹¹⁾

I reported someone on purpose because they reported me. ⁽⁹⁾

Just 14% of those children who were shut out say they were cut-off because they were detected as underage: *I used a fake age or said I was older than I am.*¹³

The same pattern holds among 12–15-year-olds who could have misrepresented their age to avoid teen protections: shutouts (45%) were driven by user reports (35%) or behaviour (30% broke a rule, 20% used bad language or were rude), and rarely by age-related concerns (15%).



Figure 2: Has a game or app ever stopped you from using your account (like being banned or blocked)? (8–12-year-olds)

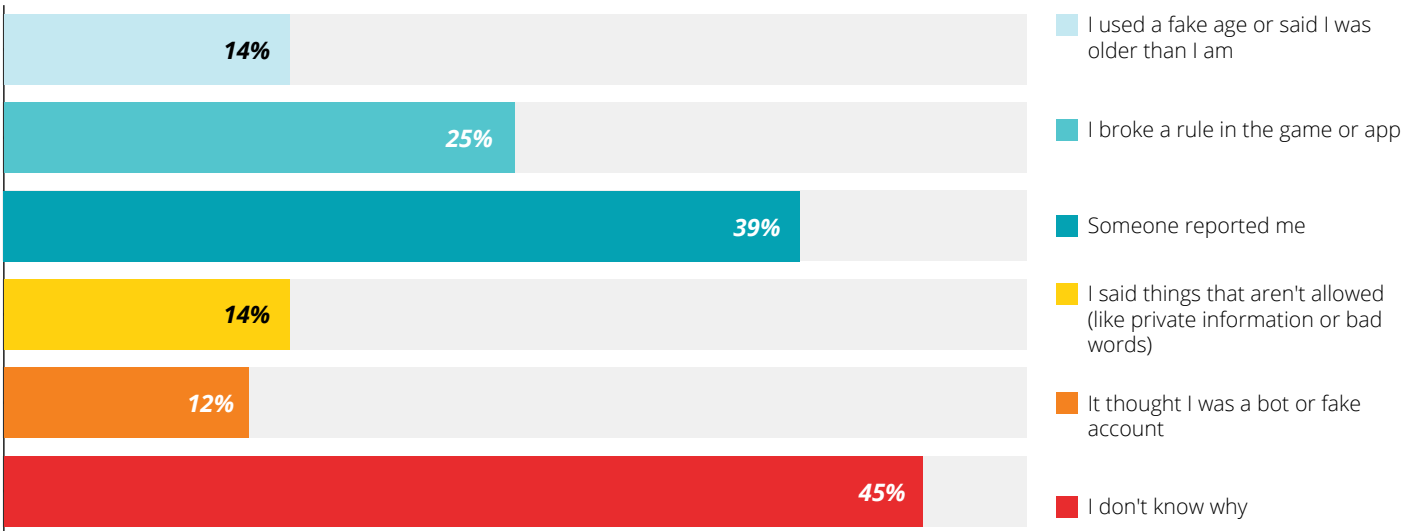


Figure 3: Why do you think the game or app stopped you from using your account? (8–12-year-olds)

8 Ref: UCD undergraduate study, in consultation with CyberSafeKids, undertaken by Harry McCormack, supervised by Dr Liliانا Pasquale, 2025-2026.

9 Such as privacy by default, restricted DMs/tags/mentions, screen time reminders, content filters, comments and downloads.

10 Safeguards for teen accounts vary by platform and may include: privacy by default, restricted DMs/tags/mentions, screen time reminders, content filters, restrictions on comments and downloads.

11 Behavioural signals could include their likes, interests, who they follow, or facial age estimation from photos posted.

12 61% on an OSC-designated platform.

13 This equates to just 4% of the overall population of children we surveyed.

This aligns with what young children told us directly in a focus group: they were unconcerned about entering a false age, even one considerably older, seeing their account closure as unlikely regardless.

This really is best described as ‘the year little changed’. In spite of industry announcements about child safety measures and new regulatory powers, children’s access remains unchanged this year. These findings show the extent to which tech companies have continued to operate in a manner inconsistent with new legal requirements since the transition period between enactment and enforcement has elapsed.¹⁴

TikTok, Meta’s Instagram and Facebook, Snapchat, and YouTube are all under investigation by the European Commission for breaches of the DSA. Preliminary findings on Meta and TikTok show serious breaches but no fines have yet been issued.¹⁵ With all of these investigations, the companies are challenging the evidence and findings by the Commission and will be able to delay payment of any fines imposed through years of litigation. It also bears stating that this approach is fundamentally flawed if it is only examining where harm has *already* occurred.

What we have detailed here is a failure by Big Tech to implement required changes that leaves children unprotected online and no safer than they were a year ago. The moral failing is that these companies continue to monetise and profit from the vulnerability of children, who can readily access these digital services that consistently deliver such age-inappropriate experiences.



¹⁴ There was a grace period of approximately nine months for the Online Safety Code between enactment and enforcement to allow for implementation of changes.
¹⁵ Non-compliance fines have been issued to Temu and X under the DSA for risk assessment and transparency failures respectively. Investigations into TikTok, Meta services, and Snapchat are at earlier stages of investigation. Under-13 access failures are among the preliminary findings by the Commission: https://ec.europa.eu/commission/presscorner/detail/en/ip_26_920.

When Safeguards Fail

Our focus now shifts from access to outcomes: what children do online, what they encounter and where, and how they navigate the challenges this presents.

Currently destroying childhood. ⁽¹⁴⁾

What Children Do Online

Given the failures of age assurance, it is of little surprise that children continue to engage with the same online activities and digital platforms as last year. This is true for both age groups surveyed. The exception to this is the rapid uptake of new AI technologies (see section *Fool Us Twice*).

I want myself to be ok online. ⁽⁹⁾

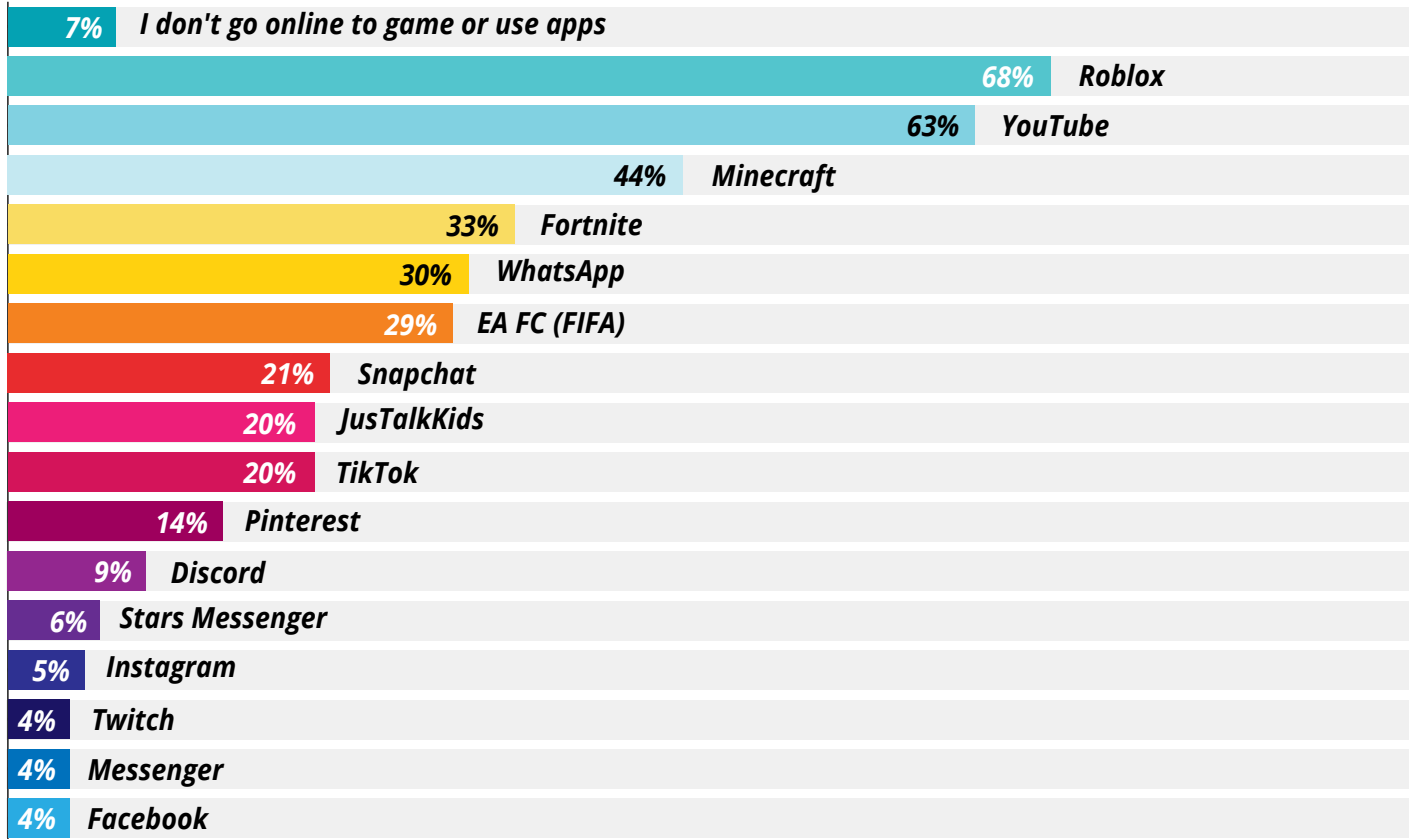


Figure 4: If you are using any of the following online **with your own account**, please tick the box beside it (8–12-year-olds)¹

¹ Children engage with a vast array of other apps and games, but they do so in smaller numbers, with other games and apps attracting less than 1% of the children surveyed.

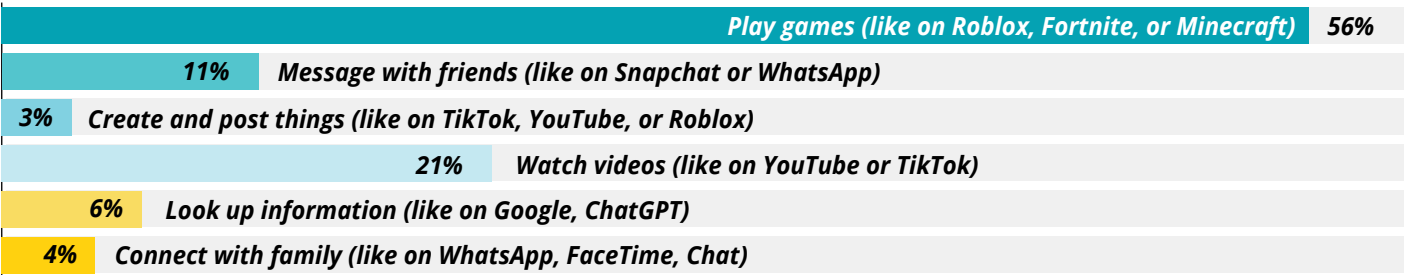


Figure 5: What do you do most when you're online? (8–12-year-olds)

For this age group, Roblox pulled ahead of YouTube last year for the first time and has maintained its position as the most popular platform for the second year in a row. Four of the top six digital services are now gaming platforms (*Roblox*, *Minecraft*, *Fortnite*, *EA FC*) and more than half of 8–12-year-olds choose gaming when asked what they do most when they go online (Figure 5).

Interest in gaming among 8–12-year-olds continues to increase year-on-year, reflecting a broader shift toward interactive entertainment and social gaming.² This underscores the need for much stronger regulatory scrutiny of gaming services than we have currently. While the DSA does apply to gaming services, none of them have been designated as a *Very Large Online Platform*³ and they are therefore not in the highest-risk regulatory tier. But unlike platforms or sites like LinkedIn or Booking.com, the user base for gaming platforms skews young. Any regulatory threshold that does not differentiate between children and adults should not be used as a barrier to providing the most rigorous regulatory oversight for digital services used by children⁴, alongside these larger digital services.⁵

Actual use of digital services may be higher than we have reported in Figure 4, given that children do not always need or use their own account to gain access.⁶ In fact, almost 1 in 4 (39%) of 8–12-year-olds access digital services without signing in or setting up their own account.⁷ Many do so because their parents have restricted their use (23%) or because they access on a device or account (28%) that is borrowed or shared, often with siblings or with a friend (Figure 6). This reality highlights one of the practical challenges of implementing a platform ban for those under-16, and why it is important to go further and pursue systemic reform of digital services.

I have stole my sister’s account. (9)

It is no surprise that among 12–15-year-olds, being online is almost universal. Just 1% indicated that they *don’t go online to use games and apps* and using multiple platforms is the norm (Figure 7).

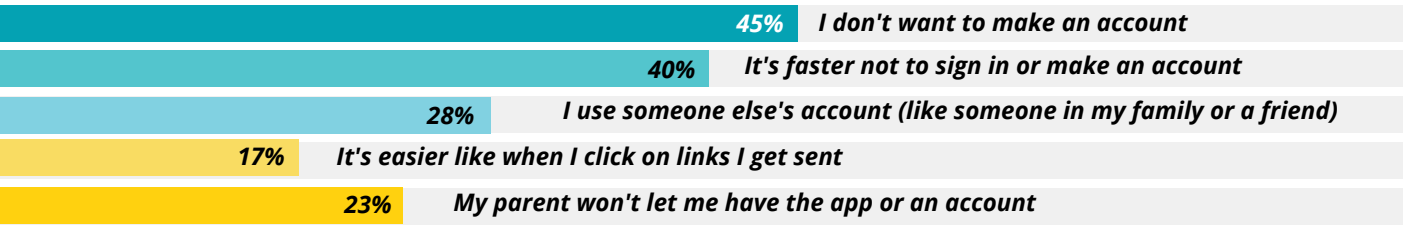


Figure 6: If you said yes, then why do you do it? (8–12-year-olds)

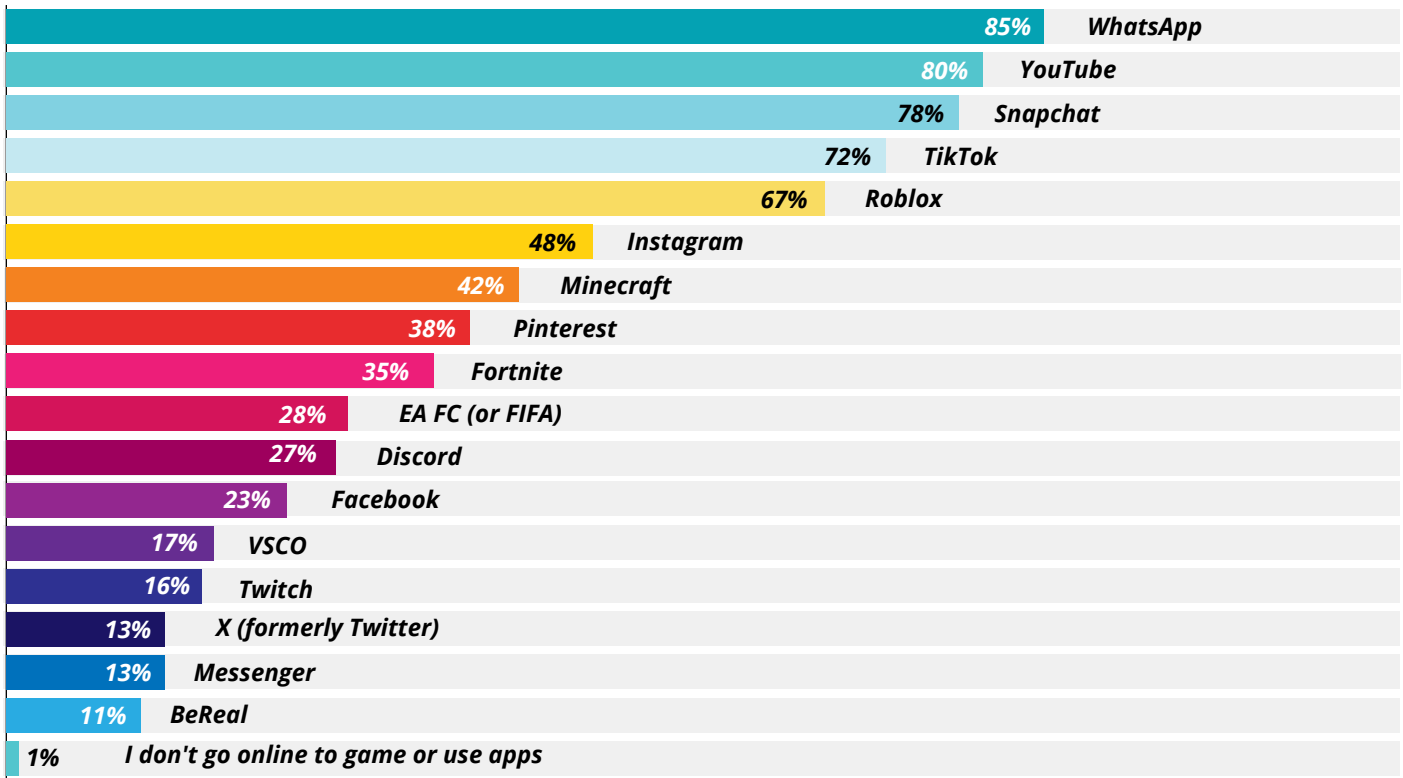


Figure 7: If you are using any of the following online **with your own account**, please tick the box beside it (12–15-year olds)

While some services are popular across all genders, there is a significant difference for some that align with their differing interests, e.g. *Twitch*, *Discord*, *EA FC*, *Fortnite* are significantly more popular with boys (Figure 8). Unlike other games, at this age, girls are more likely to engage with Roblox than boys, due to the type of social experiences on offer. X is an

interesting case too, as it grows steadily in popularity from the age of 12 (8%) to the age of 15 (17%) and is considerably more popular with boys (18%) than girls (7%); this may be linked to content interests, lower emphasis on visuals, and general tone of communication that girls tend to shy away from more.

2 Gaming trending up: 2025-2026: 48%, 2024-2025: 42%, 2023-2024: 36%.
3 The threshold set for a *Very Large Online Platform* or VLOP is 45 million monthly active users.
4 In its latest DSA disclosure, Roblox declared 48 million MAU for the 6-month period ending February 13, 2026, but there will be a delay before a decision on VLOP status will be applied. Ref: <https://en.help.roblox.com/hc/en-us/articles/13061336948244-EU-Digital-Services-Act?>
5 The most recent report from the EU Commission, *Special Panel on Child Safety Online* (July 2026), which prepares the ground for the gaming services to be considered together with social media platforms under the banner of 'social media +', is to be welcomed. For more information, see https://commission.europa.eu/topics/digital-economy-and-society/special-panel_en
6 Early reports from Australia suggest significant numbers of children under-16 access content via browsers (for which a personal account is not required): browsers are not addressed by the Australian law that prohibits the use of social media until the age of 16.
7 The question posed is: *Do you go on websites or apps without signing in or having your own account (like to watch videos or look at things online on YouTube or TikTok)?* Figure 6 is a follow on to this question.

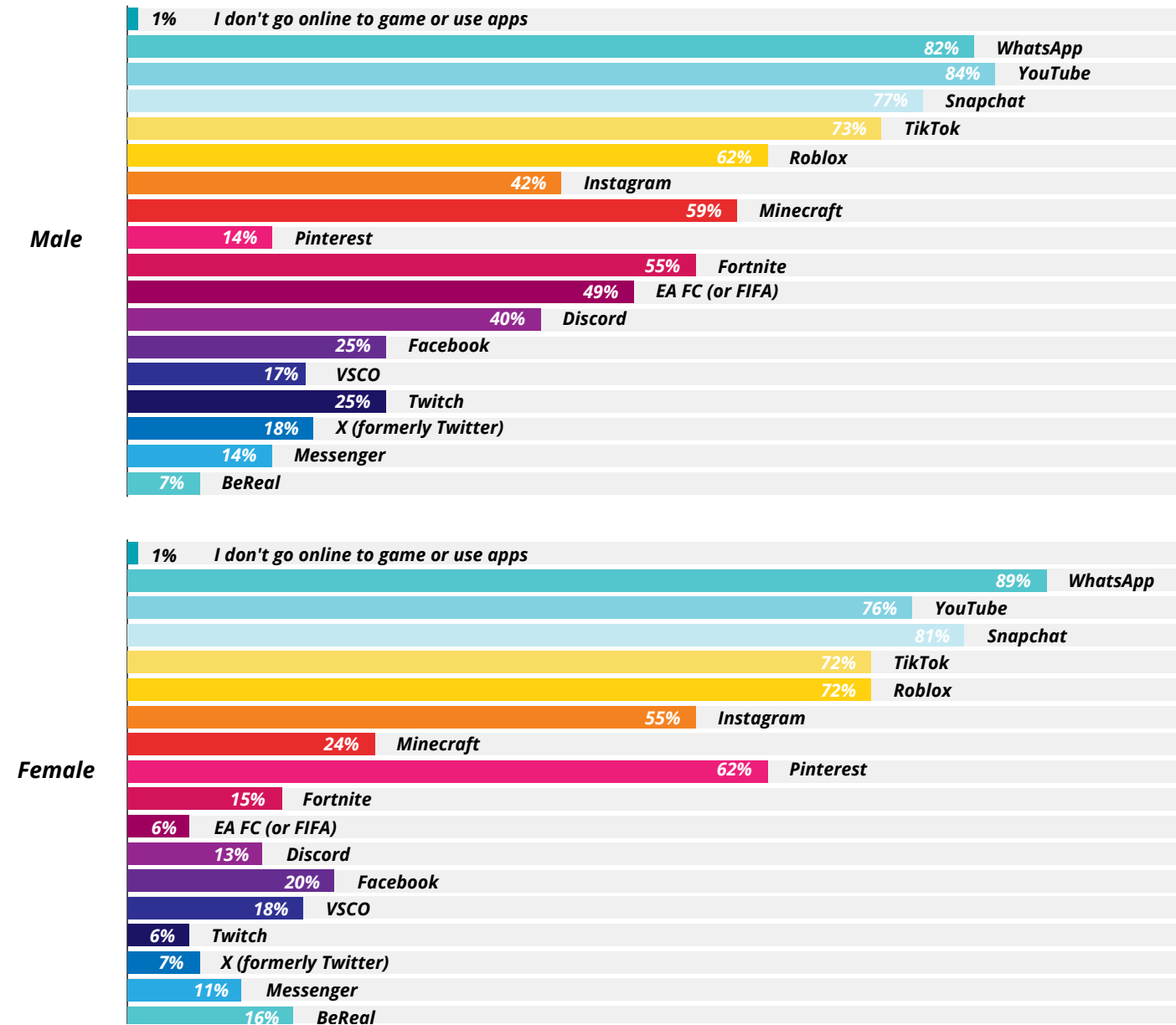


Figure 8: If you are using any of the following online with your own account, please tick the box beside it (12–15-year olds, by gender)

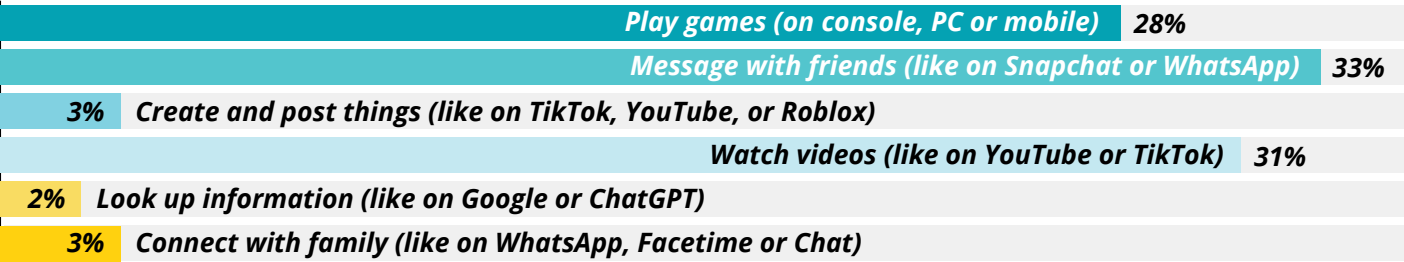


Figure 9: What do you do most when you're online? (12–15-year-olds)

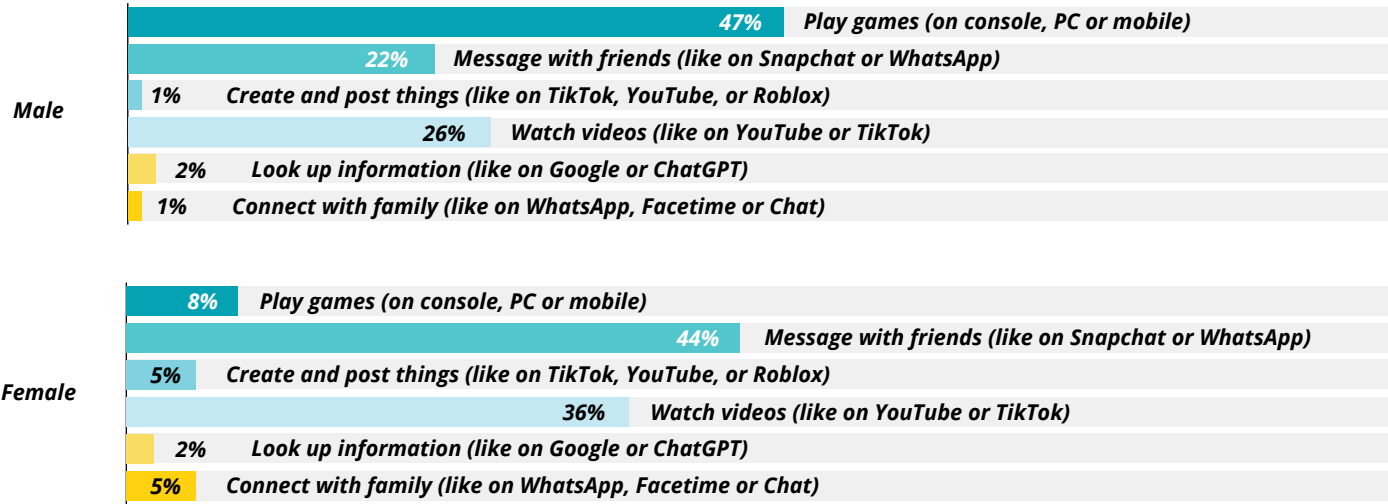


Figure 10: What do you do most when you're online? (By gender, 12–15-year-olds)

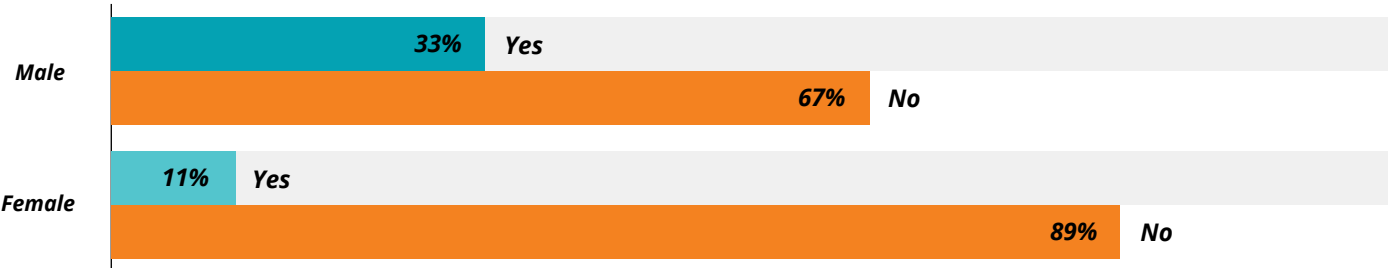


Figure 11: Have you played a computer or video game that has an age rating of over 18s in the last year? (8–12-year-olds, by gender)

There is no change in the interests of 12–15-year-olds this year. While messaging with friends and watching videos take up more time than gaming overall (Figure 9), this is the age when interests diverge by gender. Boys continue to spend most of their time online gaming in their early teens, while girls are more likely to engage with social media, either messaging with friends and/or watching videos (Figure 10).

The popularity of Roblox, Fortnite, EA FC, and Minecraft have already been highlighted but children in both age groups also play games with higher age ratings, some that are rated by PEGI⁸ as suitable only for adults – the most commonly mentioned

are still Call of Duty and Grand Theft Auto. Among 8–12-year-olds, 22% have played an 18s video game in the last year and this is far more common for boys (33%) than girls (11%) (Figure 11). This rises to 34% for 12–15-year-olds, with over half of boys doing so (51% vs. 16% of girls). There has been no reduction in access to these highly unsuitable games in recent years, with ratings used as guidance at best, and no enforcement checks, especially for digital sales. Parents often fail to realise how high the bar actually is for a game to earn an 18 rating in the first place, and focus on risk reduction in other digital environments instead.

⁸ PEGI (Pan European Game Information) is the age rating system (3, 7, 12, 16, 18) used across most European countries based on suitability of content. From June 2026, monetisation features and certain online interactions will be considered when rating new games.

What Children Encounter

Nudity, sexual content, unpleasant things. ⁽¹¹⁾

This year, the overall prevalence of negative incidents across these digital environments – games, messaging services, or social media – did not improve for either of the age groups that we survey, in spite of regulatory obligations around age-appropriate experiences for minors.

In the last year, 1 in 4 were bothered by some form of contact or content online (26% of 8–12-year-olds and 25% of 12–15-year-olds). This is described as *something that made you feel upset, weird or scared or something you didn't want to see or to be part of*. For brevity, this is referred to throughout the report as *bother*. For the older age group it is more common amongst girls than boys (27% vs. 22%). The prevalence of different types of harm children report has shifted when describing incidents that bother them however.

It is worth noting that many children who encounter misinformation, hate, or mature content do not report feeling bothered by it. When we meet and survey children we observe vastly different norms in different school communities, and even on different platforms, as to what are accepted behaviours and

A Note on Regulation: Article 28 of the DSA requires providers of platforms accessible to minors to put in place appropriate and proportionate measures to ensure a high level of privacy, safety and security.

Ireland's Online Safety Code goes further with binding rules for video-sharing platforms, with a content-prohibition obligation covering cyberbullying, self-harm and suicide promotion, eating-disorder content, hate speech, child sexual abuse material (CSAM), and terrorism content.

experiences. Repeated online exposure desensitises children, making them significantly less likely to report when encountering similar online situations. Differing levels of exposure offline can also be a factor in differing reactions. As a result, figures based on self-reported bother likely understate the true scale of children's exposure to this kind of harmful content and contact.

The findings presented below (Figures 12, 13) relate to the *type of bother* reported, and are based only on children who indicate they had experienced something that bothered them online (it is not the full sample).

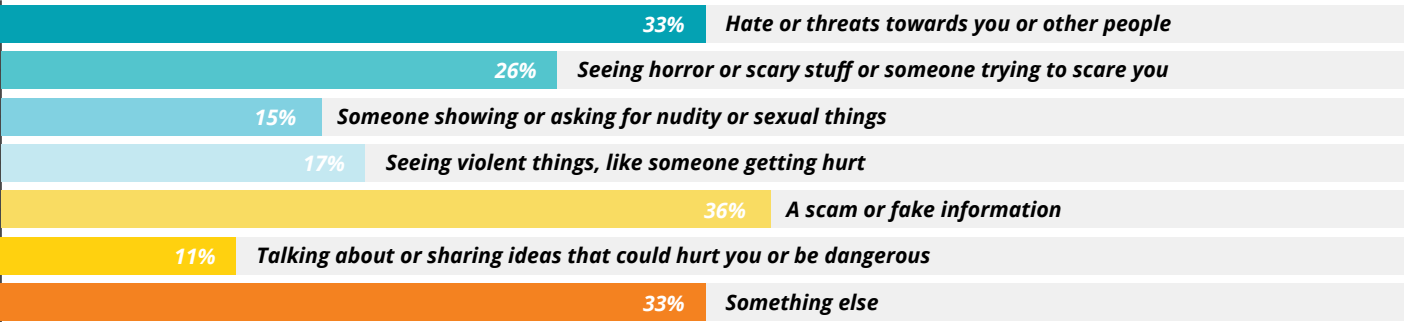


Figure 12: If this happened to you, was it... (8–12-year-olds)



CONTENT & CONTACT*



CYBERBULLYING

8–12
-YEAR-OLDS

26% were bothered by something online
24% kept it to themselves
31% reported it online

Types of experience for those affected:

36% scams and fake information (up from 25%)
33% hate and threats
26% horror and scares (down from 43%)

12–15
-YEAR-OLDS

25% were bothered by something online
34% kept it to themselves
29% reported it online
This was more common for girls (27%) than boys (22%)

Types of experience for those affected:

41% scams and fake information
(up from 29% last year):
more common for boys (46%) than girls (34%)
38% hate or threats (up from 31%):
more common for girls (41%) than boys (31%).
29% violence (up from 22%)
23% horror and scares (down from 33%)

28% were cyberbullied (up from 22%)
This was more common for boys (30%) than girls (26%)
28% kept this to themselves
31% reported it online

34% were cyberbullied
This was more common for girls (36%) than boys (31%)
Cyberbullying rises steadily with age, climbing from 30% at 12-years-old to 37% at 15-years-old

39% kept this to themselves
21% reported it online

*Comparative statistics are from academic year 2024–25



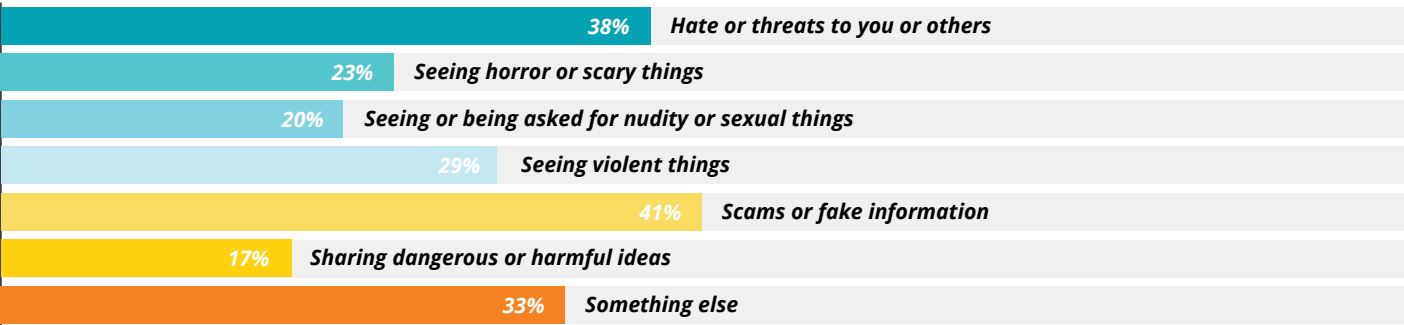


Figure 13: *If this happened to you, was it...* (12–15-year-olds)

Scams and Misleading Content

Exposure to scams, bad or fake information is now the most common cause of bother online, across both age groups, and this is up considerably on previous years: 36% for 8–12-year-olds (up from 25% last year) and 41% for 12–15-year-olds (up from 29% last year).

AI-generated content could be driving some of this, based on testimonials and focus group comments, where children discussed the prevalence of AI-slop and automated accounts.

Children are concerned about the spread of misinformation online, with older children highlighting bias in certain topics, particularly in relation to politics.

It is more common for boys to be affected than girls in the older age group: 46% vs. 34%. This could be due to a combination of factors such as their choice of digital environments (gaming platforms and forums with less moderation like X), higher-risk online behaviours (boys are more likely to have public accounts and interact with strangers online⁹), and algorithmic gender profiling.

Misinformation is spread a lot online mainly involving political information. ⁽¹⁴⁾

I was in a group and then it got hacked and a Trojan virus¹⁰ was sent. ⁽¹³⁾

Social media can be very biased in certain topics such as politics. ⁽¹⁴⁾

I truly believe I spend too much time on the internet and I think it has changed my ways of thinking in a bad way. ⁽¹³⁾

This is corroborated by a UCD study into TikTok, Snapchat, YouTube and Instagram, undertaken in consultation with CyberSafeKids this academic year, which found that *the algorithm platforms prioritise engagement over accuracy, the system is built to find what hooks you, and for many users, they can easily be hooked by fake or misleading content designed to appeal towards or against their political, moral or religious sensibilities.*¹¹

9 This year 61% of boys and 38% of girls have public account(s). 49% of boys have friends and followers they do not know vs. 40% of girls, 38% of boys game with people they do not know vs. 24% of girls.
10 This child is likely referring to the spread of malicious links via a trusted contact whose account has been compromised.
11 Ref: UCD undergraduate study, in consultation with CyberSafeKids, undertaken by Harry McCormack, supervised by Dr Liliana Pasquale, 2025-2026. Platforms audited were TikTok, YouTube Shorts, Instagram and Snapchat.

As noted earlier regarding self-reported bother, figures likely underrepresent actual exposure – children may not recognise when content is misleading or inaccurate, particularly when algorithmic funnelling keeps them within echo chambers and reinforces false narratives.

Hate, Threats and Cyberbullying

The sheer prevalence of hate and threats online this year points to children requiring a high level of resilience in order to participate in everyday digital life. Rates are consistent with last year among 8–12-year-olds (33%), but the situation has worsened among 12–15-year-olds (38%, up from 31% last year). It is also more common for older girls to be targeted than boys: 41% vs. 31%.

This is corroborated by ATU’s research into Snapchat’s Spotlight feature, conducted this year in consultation with CyberSafeKids, where it was found that *hate-speech and bullying content targeted identity groups and individuals, reinforcing hostile norms and conflict-driven interaction styles.*¹² The UCD study cited above also found incidences of targeted hate speech and racist slurs on Snapchat and Instagram served to teen accounts, even with default settings enabled.

In addition to accounts of hate speech and death threats, children also reported high levels of

cyberbullying behaviour this year. Among 8–12-year-olds there is an increase to 28% (up from 22% last year) and it is more common for boys (30%) than girls (26%) in this age group.

Just as in previous years, cyberbullying rates are higher following the move into post-primary education, with 34% of 12–15-year-olds directly affected. With the older age group girls (36%) are more likely to be cyberbullied than boys (31%). Prevalence rises steadily with age, increasing from 30% at aged 12, to 37% at aged 15.

In a review of these behaviours, exclusion is again the most common problem encountered (Figures 14, 15).

Messaging in general is a concern: 10% of 8–12-year-olds and 14% of 12–15-year-olds indicate that they have received hurtful messages. From classroom discussions and focus groups we have observed that custom digital stickers have altered how young people are communicating on apps like WhatsApp and Snapchat. While most stickers are harmless, custom stickers can act as inside jokes and in some cases are being weaponised for cyberbullying. In a focus group this year with children aged 13–17, generating stickers for later use based on an nude image shared was worryingly one of the actions considered to be the ‘norm’.

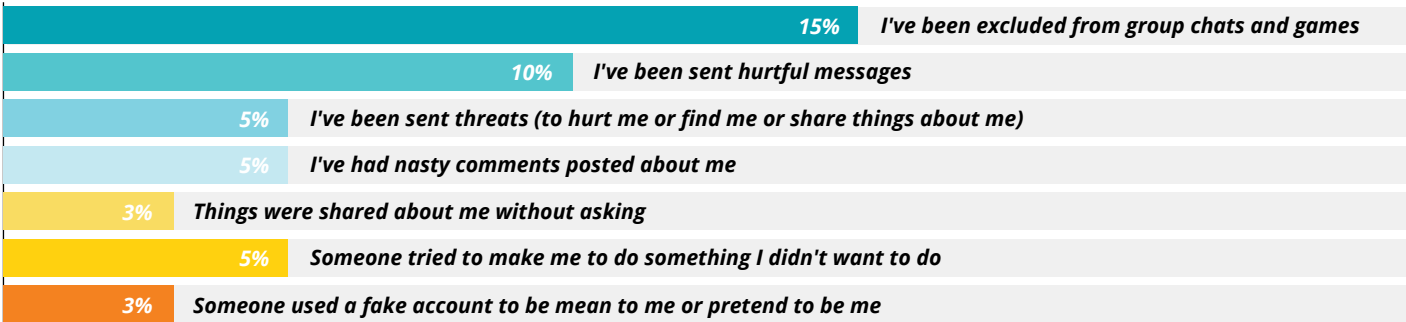


Figure 14: *Tick any of these things below that have happened to you online (this could be on games, apps, websites or messages)* (8–12-year-olds)

12 Ref: ATU Cyberpsychology Undergraduate Study – *Gendered Algorithmic Exposure on Snapchat Spotlight: An Exploratory Audit of 13-Year-Old User Profiles*. Supervised by Máire Carr, Lecturer in Cyberpsychology, ATU, 2026.

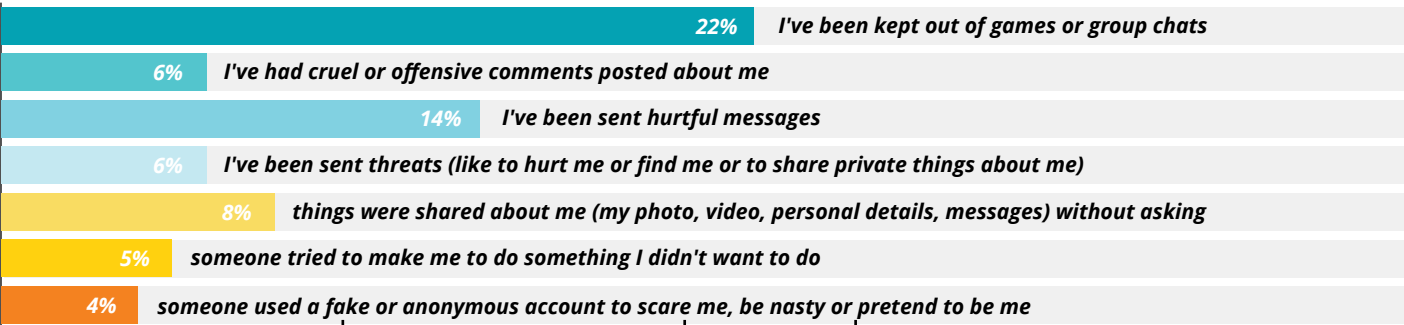


Figure 15: Tick any of these things below that have happened to you online (this could be on games, apps, websites or messages) (12–15-year-olds)

This year we have heard of impersonator accounts being set up using photos shared previously by the target or their family members, bullies repeatedly tagging a target in reposts of cringeworthy or humiliating content, and even of children being blackmailed. A fairly common issue appears to be making false reports to the platform, such as claims of underage status or misconduct, in order to get the target shut out of their accounts.

1 in 20 children report that in the last year someone tried to pressure them into doing something they didn't want to do. It is difficult to say whether that pressure was coming from peers or from online predators or some mixture of the two, but requests for 'nudes' or 'inappropriate' photos, online currency, personal details, and to move off-platform have all been mentioned in anonymous feedback this year.

Someone was being really nice to me and giving me compliments then asked me to send inappropriate pictures. ⁽¹²⁾

Somebody from another school made a TikTok page about me and got pictures off my mum's Facebook account and made fun of me. ⁽¹²⁾

A guy asked whats my name, where I am from and asked if I wanted to chat with him in Discord or Snapchat. I left the game immediately and stopped playing Among Us for a month or 2 and told a friend. ⁽¹¹⁾

Based on testimonials from children, group chats emerge again as a potential vehicle for cyberbullying, and they are more common with younger children this year than last: 72% of 8–12-year-olds participating (up from 60% last year, Figure 16).

Younger children face a learning curve when they begin using group chats. They may experience online disinhibition and are still developing their digital communication skills and learning the boundaries of acceptable online behaviour. Communicating in groups is more problematic, where social exclusion and pressure to join in unkind behaviours can occur.

My friends had a group chat without me and were talking bad about me. ⁽¹²⁾

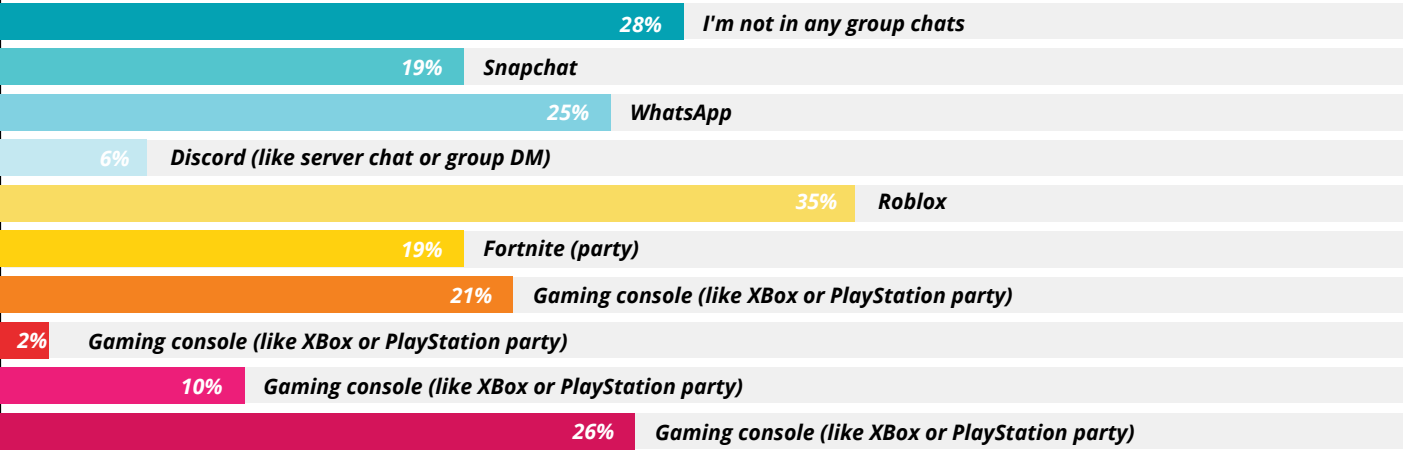


Figure 16: Which apps/games/devices do you use for group chats with classmates and friends? (8–12-year-olds)

3 girls made a post about me and sent it to the group chat and my friends because i added my friend who felt left out. ⁽¹⁰⁾

It is common to communicate in groups when gaming, so it's no surprise that 'parties' are being set up on Roblox, Fortnite and gaming consoles. 13+ messaging apps like WhatsApp and Snapchat are also used in high numbers, both of which facilitate disappearing messages that can encourage poor behaviours. In some schools we have also observed problems even when using more child-friendly messaging apps, like *Stars Messenger* and *JusTalkKids* due to that steep learning curve we mentioned previously. It is possible that these two apps make up a large portion of the *something else* category, given the popularity of these two apps (8% use *Stars* and 20% *JusTalkKids*, Figure 4) with 8–12-year-olds.

Horror or Scary Content

Seeing horror or scary content has declined significantly this year across both age groups at 26% (down from 43% for 8–12-year-olds) and 23% (down from 33% for 12–15-year-olds) respectively. While this was previously the most frequent complaint, it is now less common than

misinformation, scams, and hate speech. For the 12–15 age group, violence also ranks higher this year than horror or scary content.

There was a really scary short on YouTube about somebody being kidnapped and being held hostage. I tried to block it out but it did not work, it still scares me time to time. ⁽¹¹⁾

I saw people selling body parts. ⁽¹²⁾

Violent Content

The numbers reporting being bothered by violent content online are fairly consistent with last year's findings for 8–12-year-olds (17% vs. 20% last year) but there has been a significant increase for 12–15-year-olds to 29% this year (up from 22% last year).

I seen a video of a fella get battered. ⁽¹¹⁾

This might reflect either a higher prevalence of violent content on these platforms, increased algorithmic funnelling towards such content, or both.

There is no notable difference by gender, with boys and girls reporting being bothered by violent content in similar numbers across both age groups. Some exposure to violent content may be occurring in video games, particularly 18+ rated games, but it is unlikely they are the primary source of this exposure as that would lead to a gender gap in reporting, as boys play these games considerably more than girls.

Dangerous or Harmful ideas

There is a decrease in the number of 8–12-year-olds who report being bothered by dangerous or harmful ideas at 11% (compared with 17% last year). Among 12–15-year-olds there is a small decrease to 17% (compared with 21% last year).

Exposure to harmful or dangerous ideas (including body image, suicidal ideation, and eating disorder content) ranked second only to adult content (including violent, sexual, and horror material) among parents' top concerns this year.¹³ However, children may under-report this category of harm because they can fail to recognise when an idea is harmful or dangerous given their more limited life experience compared to adults, and following repeated exposure to similar messaging resulting from algorithm funnelling.

I saw someone hurt themselves. ⁽⁸⁾

I’ve been sent death/self harming threats saying I will hurt myself if you don’t do this or I will kill myself if you don’t do this or people telling me to kill myself or them telling me to cut deeper or for me to self harm when I

already struggle with it. ⁽¹²⁾

This is borne out by ATU’s research¹⁴ into Snapchat’s *Spotlight*, conducted this year in consultation with CyberSafeKids. Findings included that *mental-health venting content showed young users publicly disclosing distress, suicidality, or self-harm, sometimes normalised or gamified within Comments. It was additionally found that female profiles were disproportionately served weight-loss and body-image content: 28 of their 58 problematic videos (48%) focused on weight, restrictive eating, or appearance, alongside beauty and skincare content. Beauty and looksmaxxing clips normalised intensive appearance-management and multi-step skincare routines for very young users. While the ...male profile saw the highest levels of hate speech/bullying (24 instances) and substantial toxic masculinity content (13 instances), including misogynistic memes, gender-stereotyping, and dark humour around violence and abuse. Toxic masculinity content included anti-feminist and anti-LGBTQ rhetoric, trivialisation of sexual violence and child abuse, and manosphere-style Memes.*

This is indicative of a wider, cross-platform pattern, which includes Roblox (see section *Growing Up On Roblox*), as well as social media apps. Ofcom’s May 2026 research found that three-quarters of UK teenagers had encountered harmful content through social media recommendation feeds, with TikTok the most frequently cited platform.¹⁵ This aligns with our own findings that among Irish 12–15-year-olds TikTok is the most cited platform for bother, with Snapchat in second place (Figure 21). Additionally, in the UCD study previously cited, there was self-harm content observed on both TikTok and YouTube Shorts for profiles of 13 and 15-year-olds with default settings.

Sexual Harms

The numbers who report being bothered by sexual content and contact online are consistent with last year’s findings: 15% for 8-12-year-olds and 20%

for 12-15-year olds. At this age, exposure usually occurs on mainstream platforms, rather than through sources dedicated solely to pornography, highlighting that the experience children are having on these platforms is not age-appropriate.

When describing these incidents, children frequently use words like ‘weird’ and ‘inappropriate’ but this year we have also observed a significant increase in children referring to ‘nudes’.

Exposure to AI-generated sexual imagery is also a factor, as is increased awareness of AI ‘nudification’ capabilities, following the controversial introduction of Grok on X, which led to what Reuters described as a ‘mass digital undressing spree’.¹⁶

In a recent focus group conducted with young people aged 13–17, the receipt of nude images was not considered a cause for concern or unusual. The most likely action taken was simply to save that image to the camera roll or add it as a ‘sticker’ to use in subsequent communications, highlighting just how normalised exposure may have become among teenagers in Ireland.

I was in a Discord server and somebody asked someone within the server to send them nudes. ⁽¹⁴⁾

24% of 12–15-year-olds have come across sexual content online in the last year, a huge increase on

last year’s reported figure of 10% (Figure 17). In the vast majority of cases, children do not seek out this content but come across it by accident. Boys (27%) are significantly more likely to have been exposed than girls (19%, Figure 18). They are twice as likely to have sought it out (2% of boys vs. 1% of girls *saw it on purpose*) but it is being pushed more to boys than girls also (25% vs. 18% *saw it by accident*).

Sexual content is heavily advertised like the website OnlyFans, this is mainly advertised on TikTok and YouTube Shorts which is mainly used by people under 18. ⁽¹⁴⁾

Rates of exposure increase progressively with age, so that by the age of 15, 38% are exposed to sexual content online and a third (33%) of these young people indicate that it is being pushed to them (Figure 19). This closely aligns with findings from research published by the University of Galway where 37% of the 15–16-year-olds surveyed in Galway, Mayo, and Roscommon reported viewing pornography in the previous year.¹⁷

While pornography is not openly promoted through sponsored advertising on mainstream platforms, adult entertainers often post sexually suggestive content, using profile bios, links, and handles to direct users to more explicit material on other

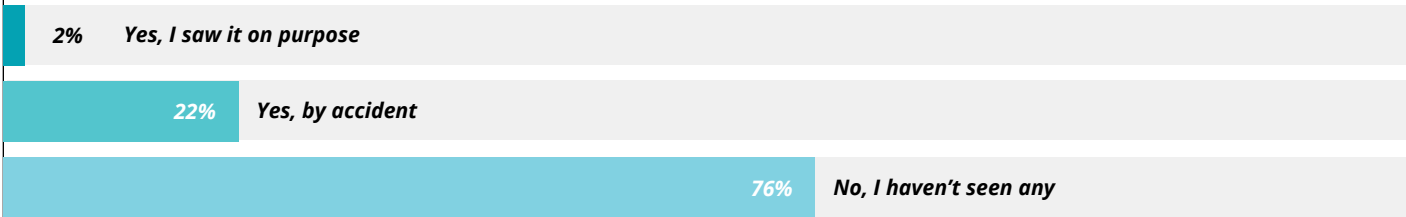


Figure 17: In the last year, have you come across sexual content online? (12–15-year-olds)

13 CyberSafeKids Parents Research (sample size 3,000+), 2025-2026 academic year
14 Ref: ATU Cyberpsychology Undergraduate Study – Gendered Algorithmic Exposure on Snapchat Spotlight: An Exploratory Audit of 13-Year-Old User Profiles
15 Ref: <https://www.ofcom.org.uk/online-safety/protecting-children/childrens-online-experiences-research-report>

16 For the formal investigation launched by the EU Commission, see: https://ec.europa.eu/commission/presscorner/detail/en/ip_26_203
17 Ref: <https://www.universityofgalway.ie/media/healthpromotionresearchcentre/conference2025/Nicola-Murphy---Pornography-use.pdf>



Figure 18: In the last year, have you come across sexual content online? (12–15-year-olds, by gender)

sites, such as OnlyFans¹⁸. This content can include implied sexual activity that occurs just off-camera. Children who engage with suggestive content when presented with it can subsequently be directed towards increasingly inappropriate material over time.

This was confirmed by the UCD study. Sexual content was served frequently to male and female teenage accounts on Snapchat (almost 5% of videos audited) and TikTok (3% of videos audited). Frequency increased rapidly in volume with continued use (i.e. first sitting (8/400 videos) to second sitting of testing (30/400 videos) on Snapchat and first sitting (4/400 videos) to second sitting of testing (20/400) on TikTok). Other platforms audited (namely YouTube and Instagram) did not serve up sexual content to teenage profiles at this level – in fact for Instagram, no incidents of sexual content were recorded in teen profiles

I was watching something and clicked someone's profile and it was inappropriate. (12)

A further risk arises through comments, where children describe encountering inappropriate comments or following commenter profiles that upset or confuse them. This is consistent with observations from the UCD study that comments

can expose 13 and 15-year-old accounts to requests for sexual content from other users: for example, *follow me and we can send*. This risk was further confirmed in the ATU Snapchat study where 13-year-old profiles were exposed to content and contact-risks through comments: *sexualised exposure often arrived via comments on otherwise benign clips (e.g. gym or beauty videos), featuring sexual jokes, fetishising remarks, references to pornography, and age-inappropriate flirtation. It determined that comment sections were a major vector of risk, frequently containing more extreme material than the videos themselves and that 'add me' and group-chat invitations appeared across content categories, indicating that Spotlight may operate as a gateway to less moderated, higher-risk spaces.*

Where This Happens

Negative experiences occur across a wide range of digital environments, including gaming, social media, messaging apps, search engines, AI tools, and streaming services (Figures 20, 21).

For 8–12-year olds, it is most common for negative incidents to occur on Roblox. Due to this alarming incidence rate (58% for 8–12-year-olds and 22% for 12–15-year-olds) and the popularity of this platform, we have a separate dedicated section where Roblox is discussed in more detail (see section *Growing Up on Roblox*).

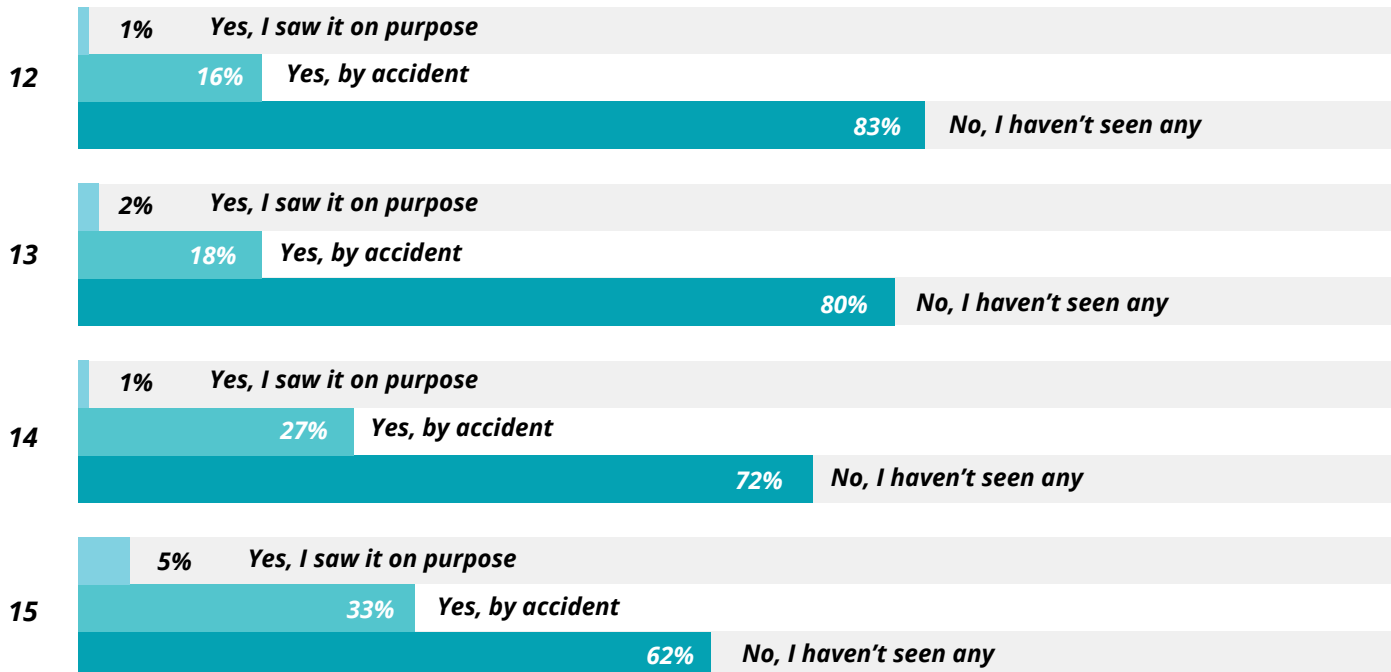


Figure 19: In the last year, have you come across sexual content online? (12-15-year-olds, by age)

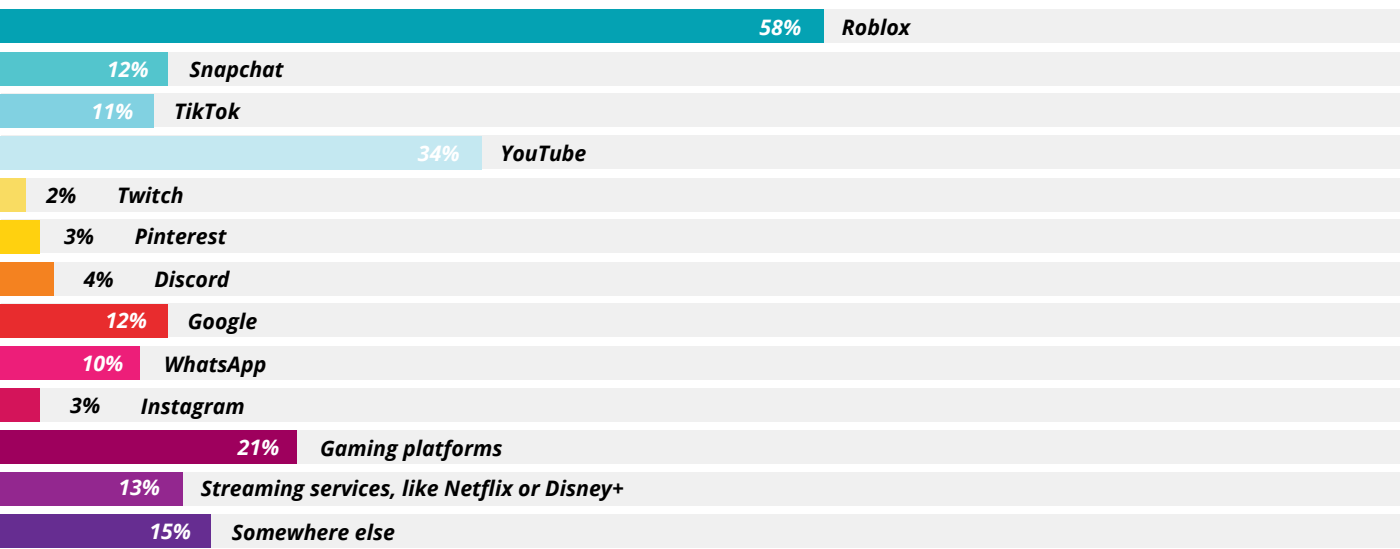


Figure 20: If this happened to you, what apps, services or games were you using at the time? (8–12-year-olds)

21% of 8–12-year-olds report negative experiences while on other gaming platforms. Toxic exchanges have been a systemic challenge across online gaming platforms for years. This is corroborated in testimonials from children. Older children are less likely to report upset while gaming, often due to the normalisation of certain behaviours after repeated exposure.

I was playing a game in Fortnite and someone told a person to die, kill himself or jump off a bridge and hang himself. (9)

¹⁸ OnlyFans is a subscription-based platform primarily associated with adult content: its minimum age requirement is 18.

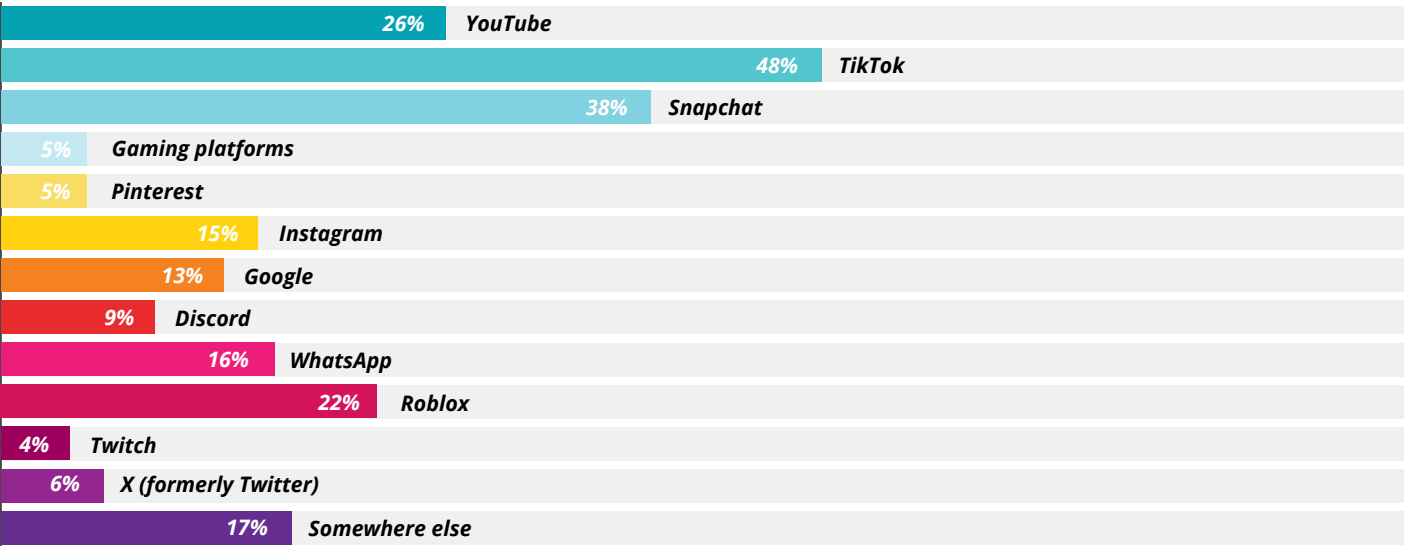


Figure 21: If this happened to you, what apps, services or games were you using at the time? (12–15-year-olds)

Someone told me on Among Us ‘I hope your family dies’. (12)

Some problems occur when gaming with friends, but worryingly 40% of 8–12-year-olds report gaming online with people they have not met in real life, and 52% have been approached by someone they do not know through games. Younger children were more likely than older children to game with strangers (40% of 8–12-year-olds vs. 31% of 12–15-year-olds), representing a pattern consistent with lower privacy awareness at younger ages, and one that leaves this age group more exposed to contact from child predators.

Some guy on Minecraft said he wants to be in my bed and sleep with me. (12)

AI sucks don’t use it. (14)

We did not include an AI option this year in this question, but (based on testimonials) it is possible that AI experiences make up some of the 15% of 8–12-year-olds and 17% of 12–15-year-olds that chose the option *somewhere else*.

Young children report exposure to inappropriate or upsetting content through browsers (12% for 8–12-year-olds and 13% for 12–15-year-olds) and on streaming services like Netflix and Disney+ (13% for 8–12-year-olds) so parents shouldn’t overlook these environments. As such, it’s important to have child profiles set up and avail of all restricted modes on every device and service that may be used by a child, and to be wary of handing over an adult’s personal device to a child, however briefly.

I was about 5 I downloaded about 10 games on my dads phone and one of them showed pictures of nudity and I deleted all of the apps. (12)

I go on Safari a lot and that’s where I see weird things. (12)

10% of 8–12-year-olds and 16% 12–15-year-olds report having problems on WhatsApp this year. This is unsurprising given how popular WhatsApp is with young people and how often they set up group chats, which as previously explained can be

very problematic – even more so on WhatsApp in fact, where disappearing messages and locked and secret chat features can be enabled. Children report being added to groups without their permission and inappropriate content being circulated. It is not known if children have additional problems with content they are exposed to via *Channels* or *Meta AI*. WhatsApp *Channels* fall within the remit of the high-risk regulatory tier of the DSA, but messaging does not and *Channels* were only added after this research was conducted. Meta announced a more restricted ‘parent-managed account’ option for under-13s in March 2026 without access to *Channels* or *Meta AI*. However, this safer version is opt-in and a child can still set up a standard WhatsApp account without any age check.

Somebody keeps on adding me to a group in WhatsApp and I don’t know how to block it properly. (9)

45% of negative incidents for 8–12-year-olds occur on a 13+ regulated platform: YouTube, Snapchat, TikTok, Pinterest or Instagram. Most commonly this occurs on YouTube (34%), Snapchat (12%) and TikTok (11%). Higher usage is generally associated with higher levels of negative incidents, suggesting the raw figures largely track exposure rather than one platform being inherently riskier. The risks themselves, in terms of content and contact, may be broadly similar across these regulated 13+ platforms.

When I tried to search something up something came up that was inappropriate and sometimes adult type of YouTube content come up. (11)

19 Under article 28 of the DSA, platforms must provide age appropriate experiences to their users, ensuring a high level of privacy, safety, and security for younger users.

Someone asked me to show weird pictures of me on Snapchat. (12)

75% of negative incidents for 12–15-year-olds occur on a 13+ regulated platform: YouTube, Snapchat, TikTok, Pinterest, Instagram or X. Most commonly this occurs on TikTok (48%) and Snapchat (38%).

Under regulation, teen safeguards must be in place but given the age assurance failures discussed previously, it is difficult to know whether safeguards are reaching children in either age group. In practice, many could be using standard adult accounts where such protections would not apply at all.

The effectiveness of these teen safeguards is called into further question by findings in the UCD study. For accounts of 13-year-old and 15-year-old boys and girls with default settings¹⁹ algorithm funnelling meant that *even with privacy settings, algorithms are designed to push engagement, not safety. This creates a pipeline where interacting with one edgy, sexual or misleading post feeds the algorithm more of the same, escalating the intensity of the content. Additionally, it was noted that for Snapchat that the friends list is a massive loophole. Once a stranger is added as a friend, they often bypass all safety filters (Direct Messages, private status, and invitations to and sending of harmful content), effectively whitelisting a predator or a bot.*

I once got a random person texting, showing me their body in inappropriate ways so I blocked them and deleted Snapchat. (14)

In the ATU study it was also determined that *Snapchat’s claim that Spotlight is moderated for a ‘13+’ audience sits uneasily with the presence of misogyny, self-harm references, sexualised comments, and aggressive bullying in content and comment threads served to 13-year-old profiles... 18.3% of Spotlight videos served to these 13-year-old profiles were coded as problematic including weight loss and body image, beauty/looksmaxxing, mental-health venting, toxic masculinity, sexual content, hate speech/bullying, and problematic comedy... harmful content still surfaced in ordinary use, suggesting that a 13-year-old following everyday interests can still be funneled toward gendered harm streams [and that] exposure patterns intersect with known adolescent vulnerabilities (e.g., body image concerns for girls, status and belonging for boys, mental-health sensitivity across genders), potentially amplifying risk even when content might seem ‘normal’ for adult users.*

In this academic year, regulation demanded that young people be provided with age-appropriate online experiences, underpinned by reliable age assurance on these 13+ platforms, but in practice this is clearly not the case and children are no safer this year than last year.²⁰

How Children Respond

When children encounter problems online we want them to reach out for help. Despite the serious nature of many of the online harms we have described, almost 24% of 8–12-year-olds tell no-one (*I kept it to myself*) when they are bothered by something online and that number is even higher, at 28%, for those who are cyberbullied (Figures 22 and 23). Just over half of them reach out to a parent or trusted adult for help: 54% if bothered, 51% if bullied. The situation worsens among older children, with 34% and 38% of 12–15-year-olds telling no-one when they encounter bother or bullying online respectively

(Figures 24 and 25). When bothered or cyberbullied, just 29% and 33% turn to a parent respectively. Similar to other years, boys are less likely than girls across both age groups to ask for help. For example, among 12–15-year-olds, boys are more likely to keep it to themselves when cyberbullied (43% boys vs. 35% girls), and girls are much more likely to tell a parent or trusted adult (38% girls vs. 26% boys).

A Note on Regulation: Both the Digital Services Act (DSA) and Ireland's Online Safety Code (OSC) require platforms to provide clear, user-friendly reporting mechanisms. Under the OSC, users must first report an issue directly to the platform before Ireland's online safety and media regulator, Coimisiún na Meán (CnaM), will consider a complaint. This reliance on platform-level reporting means that, beyond their content-moderation function, reporting also serves as a valuable source of evidence for systemic harms, provided they are easy to find and used correctly.²¹ An 'Individual Complaints Mechanism' – allowing individual users to report and have harmful content removed by CnaM if the platforms do not action this themselves – although provided for within the OSC, has not yet been implemented. Although you can report individual cases to CnaM, they cannot action removal, but complaints are noted and added to a body of evidence of systemic failure by the platforms.

In previous years we focused on offline actions in this regard, namely who children told. This year, we also asked children what actions they took online after a negative experience, such as blocking or reporting a user. This is both to understand whether children attempt to protect themselves from

future exposure, and what evidence is provided to platforms and regulators of moderation gaps and systemic harm.

In the majority of cases children across both age groups fail to report problems to the platform providers. For 8–12-year-olds, just 31% report either online bother or cyberbullying, and among 12–15-year-olds, 29% report online bother. Only 21% report cyberbullying.

With online actions we also see a gender difference, with girls more likely than boys to avail of online reporting and blocking mechanisms or to consider changing their account settings to protect themselves from future problems. For example, among 12–15-year-olds just 14% of boys say they would report the person (or account) online compared with 25% of girls who say they experience cyberbullying. Boys may be more tolerant of negative behaviour encountered while gaming, and as a result may be less likely to report

accounts or players when cyberbullying occurs during gameplay. The reactions are closer when it comes to reporting of bother, with 31% of boys and 27% of girls taking action. However, boys are less likely than girls to block the content or account, or try not to see that content in the future (25% of boys vs. 33% of girls).

This tendency to underreport may not be because reporting mechanisms are difficult to find or to use, particularly for 12–15-year-olds. In the UCD study of popular platforms – namely Roblox, WhatsApp, Snapchat, TikTok, YouTube, and Instagram – it was observed that *the report function is easy to find and you have a varied selection of grievances to report a user for including specific posts and the potential of the user being under the age of 13*. This finding aligns with testimonials received from children this year in which they frequently mention reporting and/or blocking in response to negative experiences. We did receive some comments from younger children who were unsure how to report content or contact, or who

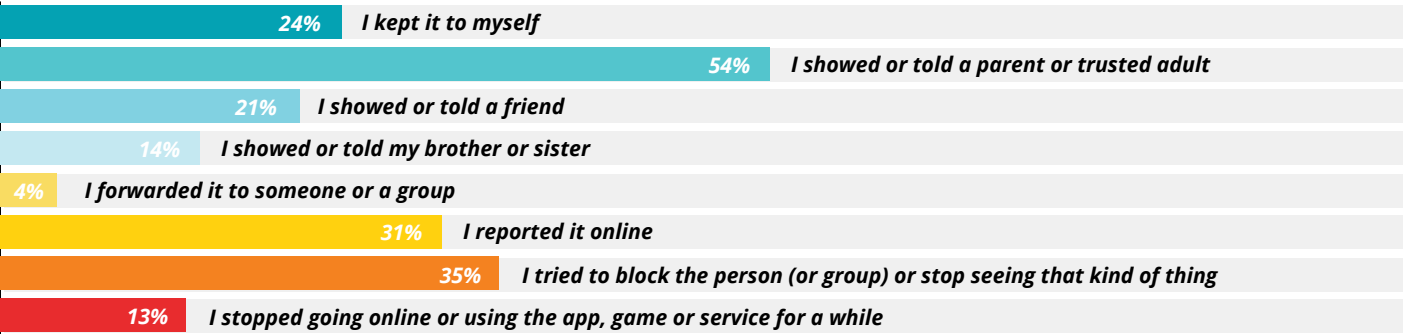


Figure 22: If this happened to you (bothered), what did you do about it? (8–12-year-olds)

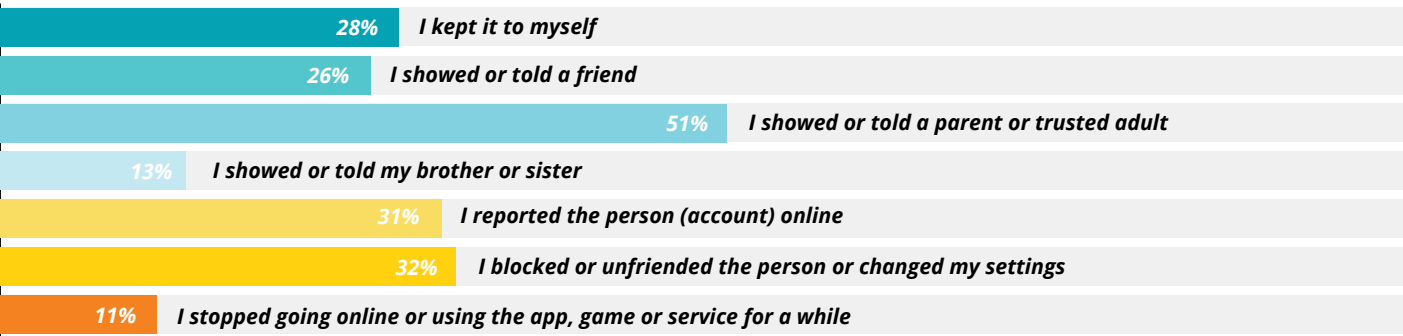


Figure 23: If any of these things happened to you (cyberbullying), what did you do about it? (8–12-year-olds)

20 EU Commission’s preliminary findings under the DSA indicate serious breaches by Meta (Instagram, Facebook) and TikTok including dark patterns, addictive design, researcher access problems, and minor’s account safety. No findings have been issued against Snapchat at the time of writing.
21 X’s complaints-handling system is the focus of Coimisiún na Meán’s first investigation under the DSA, launched in November 2025 – specifically considering the ability to appeal content moderation decisions and be informed of outcomes. Since December 2025, investigations into TikTok and LinkedIn have been ongoing and are considering anonymous reporting of suspected child sexual abuse material and ease of use of reporting mechanisms.

struggled with the settings. This is unsurprising given how many underage users are able to access these platforms. We also, unfortunately, received feedback that reporting mechanisms are sometimes misused as a way to target or exclude someone, which speaks more to broader digital norms (see section *Hate, Threats* and *Cyberbullying* above) than to the mechanisms themselves.

It is important to mention that this underreporting of negative experiences is not a failure by children. It reflects instead a flawed assumption by platforms

and regulators that children should be relied upon to identify and report harm themselves. This is the wrong way around. Real protection means preventing harm before it reaches children, not depending on them to flag it once the harm has already happened.

Whether examining what children do online, what happens to them, or how they respond, the same idea emerges time and again – failures in design and legislation are at the heart of the problem.

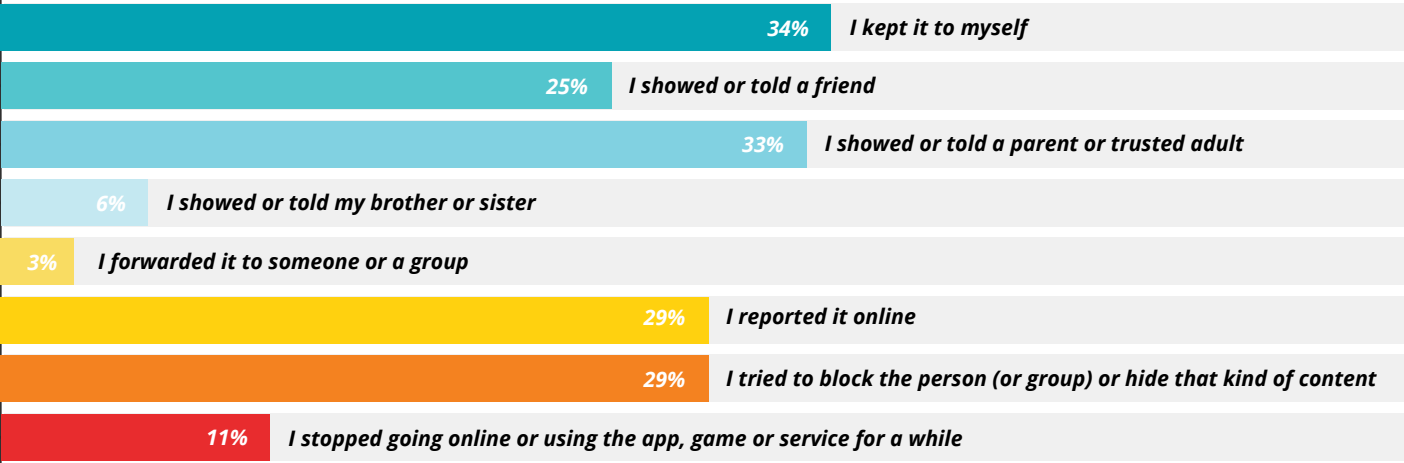


Figure 24: If this happened to you [bothered], what did you do about it? (12–15-year-olds)

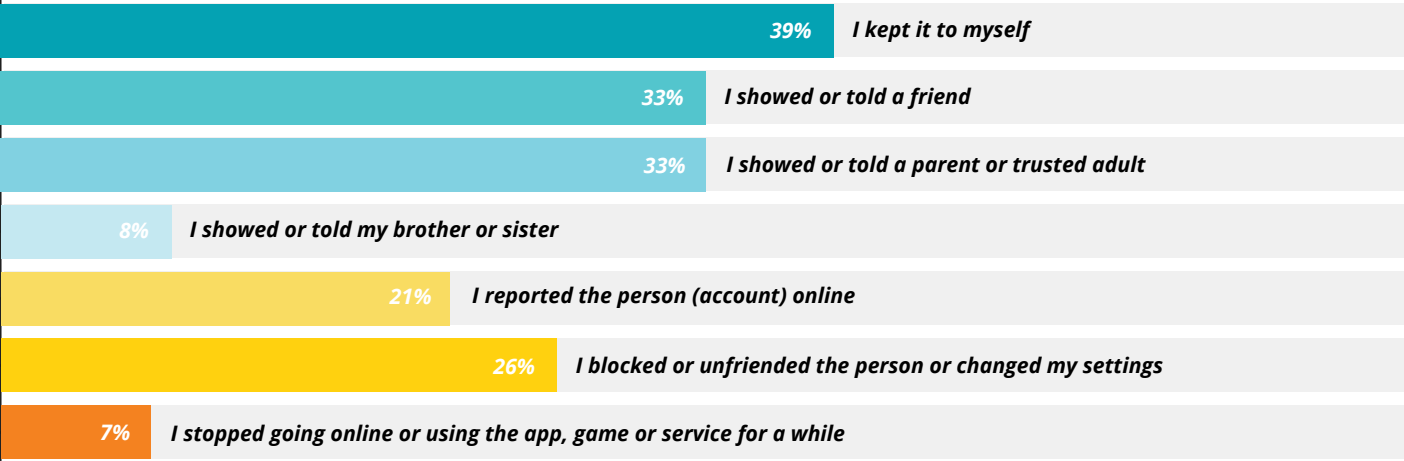


Figure 25: If any of these things happened to you [cyberbullying], what did you do about it? (12–15-year-olds)



Growing Up On Roblox

They need to make Roblox a safer place for children. There is a lot of weird adults on this game. ⁽¹²⁾

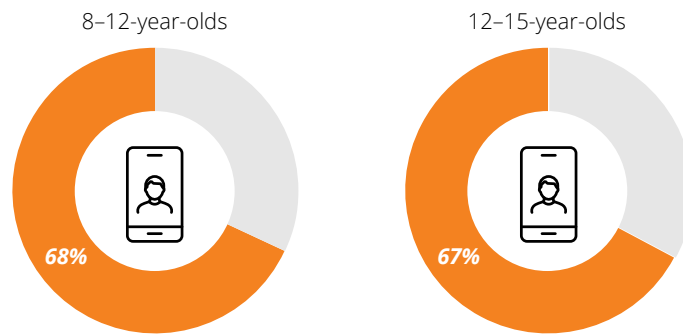
No other platform commands as much of young children's attention as Roblox – which is why it deserves its own section this year.

The primary users of Roblox are children, and those as young as five years old can create their own accounts. In Q1 2026, among age-checked users¹, Roblox reported that 35% are younger than 13, 38% are aged 13–17, and only 27% are 18 or older. While its block-based visual style appeals to young children, the cartoon-like aesthetic, with simplified avatars and environments, can also create a perception gap for adults who underestimate the breadth of experiences they may be having when they play on Roblox.

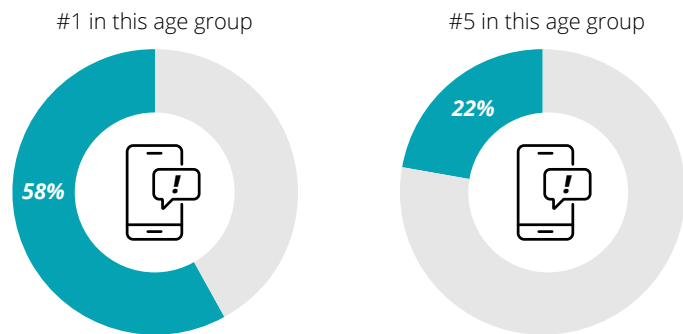
Five years ago², we highlighted that Roblox was very popular with 8–12-year-olds. 32% had their own accounts, making it the 5th most popular digital environment with this age group, surpassed only by YouTube, TikTok, Snapchat, and WhatsApp. Since then, it has grown in popularity year-on-year, while usage of these other apps has declined: Roblox now sits comfortably in first place. Its use is now so widespread at 68% adoption (69% of boys, 66% of girls), it is no exaggeration to say that it plays a defining role in shaping the modern digital childhood experience.

Many young people retain their Roblox accounts as they transition into post-primary education. 67% of 12–15-year-olds use Roblox (62% of boys, 72% of girls). Shifting game preferences and access to voice chat at age 13 provides more opportunities for social interaction, potentially explaining the greater interest among girls. At this stage in their lives, young people tend to adopt a range of social media apps, which may impact on the amount of time this older cohort of children spend on the platform.

Have accounts on Roblox



Where negative incidents happen*



*Of those who reported being 'bothered' online.

¹ In 2021 Roblox introduced an optional age-verification system to unlock features such as voice chat. From January 2026, users globally must complete an age check in order to access public chat and in-game direct messaging. Many users have yet to verify their age but for those who have, Roblox reports that users skew younger than previously reported.
² Ref: CyberSafeKids, Annual Report, 2021-2022.

It is misleading to describe Roblox as a ‘game’. It is an online platform that enables game creation and hosts user-created games and other interactive experiences that fall outside the conventional definition of a video game. Roblox refers to the user-created content on its platform as Experiences rather than games, reflecting the broader range of activities available beyond conventional video games.

A staggering 58% of the 8–12-year-olds who reported negative experiences online this year say the incident took place while playing Roblox, making it by far the most commonly cited online environment³ (Figure 20) for this young age group. 22% of 12–15-year-olds also cite Roblox. These incidents related to a mixture of content-related, contact-related, and commercial-related harms.

Content: The Experiences

There are a lot of weird apps on Roblox that can put me on edge like Brookhaven or Life Together. ⁽¹¹⁾

In Roblox people were cursing and using guns I showed my parents and left the game. ⁽¹¹⁾

I saw a video of bad moderation in Roblox. I saw stripper clubs some random guy doing the susy on a girl who tolerated it and even like doing it. ⁽¹⁰⁾

Roblox hosts an active pool of around 16 million unique games/experiences⁴. Children in the youngest category (5–9 year olds) by default get access to games with a maturity rating⁵ of *Minimal* or *Mild*. We found that *Minimal*-rated role-play experiences such as *Brookhaven*, *LifeTogether* and *Berry Avenue* are firm favourites with young children. Other frequently cited experiences include *Blox Fruits*, *99 Nights in the Forest*, *Grow a Garden*, *Adopt Me*, and *Dress to Impress*, all of which are available to the youngest of Roblox users, while the *Moderate*-rated *Murder Mystery 2*, available from age 9, is also occasionally mentioned.

With a platform of this scale that has millions of user-created games and interactive experiences, moderation of content and categorisation of Experiences will always be a problem. Mislabelled Experiences allow children to access highly problematic content today. Additionally, very young children have reported being upset or confused by thumbnails and other descriptors for *Restricted*-rated and *Moderate*-rated games they are prohibited from playing, but which still appear when they are browsing through Experiences. This is an unnecessary design feature that increases exposure to upsetting content and could encourage a curious child to seek out ways to bypass age restrictions, or to watch gameplay videos on a video-sharing platform.

Exposure to unsuitable content can start off-platform and may not necessarily be related to the platform’s recommendation algorithm. Children report seeking out games that they became aware of off-platform, e.g. through watching gameplay videos on video-sharing platforms or if they see a title discussed in a Discord community group.

In an observational study carried out by ATU cyberpsychology undergraduates, in consultation with CyberSafeKids, it was found that *parental controls blocked access to Experiences correctly tagged*

as Moderate or Restricted, but they did not prevent exposure to harmful content in mislabelled or poorly categorised games, nor to inappropriate public chat, avatars, thumbnails, or algorithmic recommendations. In addition, they found that *many sexualised or disturbing Experiences, including role-play spaces and mental-health themed games, carried a Minimal rating and were accessible to 5-year-old accounts even with parental controls switched on and that thumbnails and avatar designs depicting substance use, suicide, or hyper-sexualisation were visible to child accounts.*⁶

Under parental controls on Roblox access to sensitive issues is disabled for younger users and this is described as *games that focus on sensitive social, political, or religious issues like immigration or abortion.* However, the ATU study found that *emotionally and developmentally inappropriate material (e.g., paedophilia debates, gun violence, abortion, extremist references) surfaced in debate-style games and via thumbnails that bypass AI moderation.*

Mental and behavioural health is not mentioned as a sensitive issue, even if this is the main or sole focus of the Experience but we found that Roblox hosts unregulated and potentially harmful Experiences, including psychological and developmental assessments like *How Depressed are you?* or *The Autism Test* and AI ‘therapists’. Many of these are *Minimal*-rated. Whatever disclaimers may be built into the profile of these Experiences, vulnerable children may engage with the advice and may in some cases be exposed to upsetting disclosures by others. A worrying finding in ATU’s observational study was that *children’s avatars encountered explicit or disturbing mental health and trauma disclosures (e.g., suicide, self-harm, abuse, sexual assault) in AI “therapy” and venting games such as Are You OK? and SKINS Therapy, often with no clear boundary between roleplay and real distress.*

Under parental controls it is possible for a parent to block individual Experiences but this does not scale well in an environment with literally millions of them, and it appears from parent reports that Roblox has capped this blacklist setting at 100. It would be preferable for a parent to create a limited library⁷ of Experiences that their child could see or play, similar to that provided by Steam Families or YouTube Kids.

Contact: The Players

I was in Roblox a guy told me let’s get freaky in the bushes, I left the game and reported him. ⁽¹¹⁾

I saw a person gooning⁸ so I banned them. ⁽¹⁰⁾

On this platform a child’s social experience isn’t solely shaped by their choice of game but also by the other players that are present in the server they are placed in when they join that game⁹. The visual content of Experiences may feel safe but the interactions enabled and the behaviours of some players are not.

In recent years, we have observed that for many young children Roblox provides their first opportunity to interact with others online, whether those interactions are with offline friends or with people they have not previously met. This particularly vulnerable younger demographic lacks both the digital communication skills and the resilience required to manage the social dynamics and recognise manipulative practices.

3 See Figure 20: YouTube is closest at 34% in spite of similar adoption numbers to Roblox and no other platform comes close to these two.
4 44+ million is the total pool but there are in the region of 16 million Experiences active.
5 Maturity ratings are *Minimal*, *Mild*, *Moderate* and *Restricted*. Under-nines can by default play *Minimal* and *Mild*-rated games, all users over nine can also play *Moderate*-rated, only those who are 18 or over can play *Restricted*-rated.

6 Ref: Inappropriate Content on Roblox: An Observational Study of Exposure and Limits of Parental Controls, Cyberpsychology Undergraduate Programme, Atlantic Technological University, 2025-2026. Supervised by Máire Carr, Lecturer in Cyberpsychology.
7 Allowed games under content settings today refers to additional games that a parent has unlocked, which by default their child couldn’t play because of their age.
8 Originating in adult internet subcultures, ‘gooning’ refers to prolonged, trance-like masturbation to explicit online content.
9 Each Experience or game can have many server instances and each server contains a group of players.

A girl (or boy) came up to me in Roblox and asked me many personal questions and it sounded like a creepy old man cause he was typing really fast. He or she asked me to meet up in real life so I left. ⁽¹²⁾

I was playing Brookhaven, there was a weird guy talking to a girl and he was being very rude and threatening to her saying things like he will hurt her and find her. ⁽¹⁰⁾

I was playing a hospital game when the man said to operate on there and I think that meant a private body part and I have seen words like babe honey and sugar pie in chat. ⁽¹⁰⁾

This guy on Roblox tried to add me. I did not know him. He said add me or you are gay. It made me feel uncomfortable. ⁽⁹⁾

I saw someone in Roblox with a shirt that said women rapist and I didn't know how to report. ⁽¹¹⁾

A random person came up to me and my friend in Grow a Garden and started flirting with one of my friends from my old school and kept asking for her to friend them and were calling her avatar cute and other weird stuff. ⁽¹⁰⁾

I saw a guy trying to nude a girl in Brookhaven. ⁽¹¹⁾

Me and my sister were playing a game, someone took us into their house and would not let us leave. ⁽¹⁰⁾

People are online dating in the 9-12 age category in Roblox. ⁽¹¹⁾

A stalker kept chasing me so I had to leave. ⁽⁹⁾

Roblox has faced widespread criticism, regulatory complaints¹⁰ and litigation¹¹ concerning allegations that bad-actors have used the platform to contact and groom or exploit children and that it has allowed the platform to become a haven for predators, while continuing to market it as safe. Certainly ATU's findings were that in-Experience chat was a major exposure channel: under-13 users cannot use DMs by default, but can read and write in public chat, where harassment, sexualised talk, self-harm encouragement, and off-platform contact invitations were observed.¹²

Roblox introduced changes to communication mechanisms in January 2026 to close down this potential source of exposure and reduce the likelihood of younger children being exposed to potentially harmful interactions with adults. All users must now complete age verification before accessing public chat and in-game direct messaging (called 'whispering')¹³. Following age verification, users can only communicate publicly or through whispering with others in the same or an adjacent age category.¹⁴ However, age categories do not create separate server instances; users of different ages may still join the same server, but will not see each other's messages in the public chat or be able to whisper to one another. Direct messaging outside of a game is locked for users under-16 (unless enabled by a parent) and for under-16s is restricted to Trusted Friends.

These new age-based communication restrictions cannot entirely prevent the transfer of social norms between age groups because children can communicate with those in adjacent age groups, e.g. a child age verified as 9-12 can communicate with children as young as 5 and as old as 15. Children

who interact with older peers may adopt vocabulary, slang and conversational norms¹⁵ that are then reproduced in interactions with young peers in the same Experience, even where platform safeguards filter some content.

While Roblox's age-based communication restrictions are a positive step, they crucially do not eliminate all forms of player-to-player communication within individual Experiences because players are not gated into different servers. This vulnerability was apparent in testimonials received from children this year describing harmful interactions through avatar proximity and social signalling such as avatar movements and emotes, drawing features, displaying items, and other in-experience methods of communication. This was further discussed in a CyberSafeKids focus group held in May 2026, several months after the rollout of Roblox's new child safety measures.

Firstly, we found that only one of the group had actually gone through the steps to be age verified by May 2026. This child mentioned that the facial estimation was off by 2 years, although the outcome in her case meant she was still in the correct age band (9-12 years). Slow uptake may be driven by safety concerns; we are often asked by parents whether allowing Roblox to facially scan their children for age verification is safe. Some of the children had noticed no change to their social experience because the public chat had previously been disabled by their concerned parents.

The children were quick to point out that because they are still placed in a server with people of different ages, they are still being exposed to inappropriate communication and behaviours.

10 Ref: *FTC Investigation Demand by Child Safety Advocacy Organizations, including Fairplay and the National Center on Sexual Exploitation*, May 2026. In the EU, the Dutch regulator, ACM, launched an investigation in January 2026 under article 18 of the Digital Services Act.
11 Ref: Federal Multidistrict Litigation (MDL) - *Roblox Corporation Child Sexual Exploitation and Assault Litigation* (MDL No. 3166) - involves 170+ active lawsuits. There are also a number of state-level government lawsuits pending (Arkansas & Oklahoma, Texas & Iowa, Los Angeles County) Settlements were reached with Nevada and Alabama and West Virginia in 2026.
12 Ref: *Inappropriate Content on Roblox: An Observational Study of Exposure and Limits of Parental Controls*, Cyberpsychology Undergraduate Programme, Atlantic Technological University, 2025-2026.
13 In-game direct messaging for users under 13 is locked by default but can be enabled by a parent.
14 Age categories are under 9 (ages 5-8), 9-12, 13-15, 16-17, 18-20, and 21+.
15 Older users may be more likely to employ euphemisms, coded language or workarounds that evade moderation.

They explained how in Brookhaven, players were communicating through customisable signs and using other in-world text features, like chat bubbles that appear above avatars. While these tools are intended to support creative roleplay and social interaction, bad actors are using them to interact inappropriately, sometimes with younger players. This is a long-standing practice, in order to bypass moderation of their messages in the public chat, and this has not been addressed by the solution Roblox provides today.

Some of the most problematic interactions children report occur in *Minimal*-rated role play games, where they may witness or directly experience inappropriate, threatening and sexualised behaviour from other players. This year children report being chased, stalked, imprisoned, threatened, propositioned and encouraged to strip in these role-play games, rated suitable for users as young as 5-years-old. They have encountered avatars dressed in highly sexualised ways and witnessed players performing sexual acts on themselves or one another. Bad actors have found workarounds to Roblox's guidelines and filters that block sexualised content and clothing from the avatar shop, exposing young players to these themes.¹⁶ Children also commented on what they termed e-daters, dating seemingly being a common feature of the platform.

A solution that children employ regularly in such cases is to leave the game and rejoin, hoping to be placed in a different server instance with different players. But this is an insidious form of harm, that causes a gradual loss of innocence. Vulnerable children with limited life experience, through repeated exposure to harmful behaviours and content, can become desensitised to the point where those behaviours are perceived as normal, acceptable, or even expected and may make a child

more vulnerable to exploitation. Some children's testimonials this year include sexual terms (e.g. rape) and slang (e.g. gooning) that would previously have been unfamiliar to most children their age, reflecting the influence of their online environments.

ATU's research corroborates children's testimonials, finding that *sexualised roleplay, AI intimacy, flirting, sexting references, discussions of pornography, and in-game emotes used to signal sexual acts were observed in public spaces and in Experiences like Boys and Girls and Boys and Girls Pool Roleplay. They found that the Roblox environment mirrors the lower tiers of the 'pyramid of sexual violence', with pervasive sexist, racist, and sexualised content that normalises harmful attitudes and behaviours.*¹⁷

Roblox has been vocal about its interest in growing its adult user base (18–34 years), which monetises 50% higher than the under-18 cohort¹⁸, due to their higher purchasing power for virtual items and creator-driven economies. Since 2023, it has hosted mature social spaces rated as *Restricted* and only available to adult users (17+)¹⁹. This can blur the lines for older users on accepted social behaviours and norms – such as flirting – because the same users continue to participate in *Minimal*-rated Experiences with children on the same platform.

Problems children report do not always relate to interactions with strangers or with those in other non-adjacent age groups: peer-to-peer bullying and harassment are also common. These problems are not isolated to Roblox, but rather something children often encounter online, especially in gaming environments. As Roblox can often be a child's first experience of communicating in an online environment, they are still developing the digital and social skills needed to engage appropriately. While some children report temporary bans based on poor behaviour,

others report failures to moderate the public chat effectively, where euphemisms, coded language and workarounds are employed. ATU's observational study corroborates moderation failures stating, *the moderation stack (AI plus outsourced human review) failed at scale; users routinely bypassed filters with spelling variants, symbols, and emotes.*²⁰

Social features of the platform, like direct messaging and group chats, can be challenging to navigate, even within trusted friendships. Private messaging and group chat (Roblox Party) is not available for users in the 5–8 category, but for the 8–12-year-olds we surveyed, most of whom should be in the 9–12 category, the Roblox Party facility is proving to be very popular. 35% of 8–12-year-olds this year have group chats on Roblox, making it the most popular place for group communication²¹ this year, and group chats can be associated with increased feelings of exclusion and higher rates of cyberbullying (see section *When Safeguards Fail*).

Commercial: The Microeconomy

Roblox has its own microeconomy, built around the virtual currency Robux, where users can buy items, trade virtual goods, and participate in creator-driven marketplaces. For younger children, with low financial literacy, this presents a steep learning curve. Many don't understand the relationship between money in the physical world and this virtual currency, so the value of digital items and what constitutes a fair trade can be quite confusing.

The platform's trading systems can expose children to scams, particularly through offers of free Robux or rare items in exchange for personal information or their account credentials. Children report being locked out of their accounts – usually through an unauthorised change of password – as the perpetrator attempts to strip their Robux and

inventory²². Roblox employs fraud protections to prevent rapid account stripping but a child's often modest balance may mean thefts won't trigger these security red flags. Importantly, these safeguards do not apply to trading systems within popular Experiences like *Blox Fruits*.

The visual content of child-favourites *Blox Fruits*, *Adopt Me* and *Murder Mystery 2* may be safe, however, the barter economy they contain can be confusing and lead to a feeling of being cheated or scammed at a time when a young child will struggle to understand the aggressive trading mechanics and peer-to-peer bartering involved. There is a knowledge imbalance when young users are trading with older ones that can leave them feeling manipulated or pressured. In these kinds of Experiences, children with limited financial means who are seeking high-value items are vulnerable to phishing scams and may agree to go off-platform for communication or to check high-value lists.

Children also report being exposed to persistent, distressing or emotionally manipulative disclosures in *Minimal*-rated donation Experiences, such as *Please Donate*, intended to encourage spending. Features within it, like displaying messages on a stand/booth or signalling using avatars and emotes, enable communication that bypass age-gated communication methods.

Too Little, Too Late

Safety concerns are often overlooked in gaming environments, as public attention remains focused on social media harms. Under the EU's Digital Services Act (DSA), no gaming platform has been designated as a Very Large Online Platform (VLOP). This means that while gaming platforms are subject to the general requirements of the DSA, they do not fall within the highest-risk regulatory tier.

¹⁶ For example, uploading custom User-Generated Content (UGC) textures that mimic revealing adult outfits or skin-toned layering.

¹⁷ ATU Cyberpsychology Observational Study: 44% of all codes (123/280) mapped onto the pyramid of sexual violence tiers (prejudiced attitudes, sexual jokes and innuendo, verbal harassment, and simulated sexual behaviour), often in games rated as suitable for 5-year-olds.

¹⁸ Ref: <https://about.roblox.com/en-au/newsroom/2026/04/roblox-fuels-high-fidelity-games-over-18-players-increases-qualifying-devex-rate-42>

¹⁹ For example, CEO and co-founder of Roblox, David Baszucki, controversially suggested that having virtual dating spaces for older users on Roblox could help end loneliness, on the Tech Stuff podcast. <https://open.spotify.com/episode/4YW2cYqRprKx4i5a1dxH81>.

²⁰ Ref: *Inappropriate Content on Roblox: An Observational Study of Exposure and Limits of Parental Controls*, Cyberpsychology Undergraduate Programme, Atlantic Technological University, 2025-2026.

²¹ The next closest is WhatsApp at 25%.

²² A further potential risk is that a bad actor who compromises an already age-verified child's account could exploit that verified status to interact with other children undetected.

People on Roblox using cheats to say cuss words. (10)

I bully children on Roblox because it’s funny and scam them. (12)

I’ve been scammed off my Roblox account a lot of times because I keep joining fake links which I think are real. (12)

So this hacker said he was the owner of my favourite Roblox game and said if I gave him my account password they would give me 100k Robux so I did, now I can’t log in any more. (11)

I was playing pls donate²³ and someone was like my whole body is broken and my dad will beat me if I don’t get more robux so I knew he was lying bcs bros thumbs would have been broken. (12)

I got threats from my friend who wanted my robux. (9)

This person was calling me a show off because he traded me on a game (mm2²⁴) and I accidentally tapped something on my screen and then I unaccepted the trade and then they started to get a lot of people to gang up against me and then they were laughing at me calling me poor and I was not wanted and I could never be a good person. (11)

23 *Please Donate* is a popular social Experience where a player can provide Robux to another player.
24 *Murder Mystery 2* on Roblox is a popular survival Experience involving One vs. All gameplay.

Consequently, they are subject to fewer regulatory obligations and are not directly supervised, investigated, or sanctioned by the European Commission. Roblox is no exception, despite the very young age of its primary user base, so it does not have to carry out an annual risk assessment, undergo an independent audit or make platform data available to researchers for the purpose of studying systemic risks²⁵, which the VLOPs and also the *Very Large Search Engines* (VLOSEs) must do.

In its latest disclosures of user numbers under the DSA, Roblox has exceeded the required threshold of 45 million monthly active users in the EU, so Roblox could be the first gaming environment to enter this highest-risk tier. However, there is likely to be a delay before any formal designation of Roblox as a VLOP is made by the EU Commission. In the meantime, Dutch regulator ACM²⁶, continues to hold responsibility for supervision and enforcement and has launched a formal investigation into Roblox as of January 30th 2026, under Article 28²⁷ of the DSA, to consider whether its current safeguards are sufficient to protect minors.

25 Obligations are outlined in Articles 34–42 of the EU Digital Services Act
26 Roblox’s EU legal representative is based in the Netherlands, making the Dutch Regulator ACM (Authority for Consumers and Markets) responsible for investigating the platform. The European Commission is not responsible for supervision until such time as Roblox is formally designated as a VLOP.
27 This stated that ‘providers of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors on their service’.
28 Roblox reported having 132 million active users in Q1 2026.

While we await the outcome of this investigation with interest, the situation appears clear to us today – existing safeguards are insufficient to the task of protecting children on a platform that hosts millions of *Experiences* and millions of active users²⁸, many of them very young children.

In spite of the age of its primary users, Roblox is not always designed with child safety in mind and recent, highly publicised changes to communication mechanisms may provide parents with a false sense of security. The fact remains that *Experiences* are far too often mis-categorised (e.g. rating role-play Games as *Minimal* despite the propensity for inappropriate conduct and creative communication methods) and safeguards do nothing to address harmful norms and interactions within *Experiences*, when servers are not strictly segregated by age group. The result is that, while some communication risks have been reduced, for this generation of Roblox users, childhood innocence continues to be eroded.



Fool Us Twice

I can easily access ChatGPT and other AI websites and you guys are not doing anything to help the kids but you all still allow AI use in the school. Genuinely one of the worst things I've seen online is people killing themselves or hurting themselves online because of AI like Character.ai and more. (13)

In contrast to the lack of impact that regulation has made on the digital landscape, there is one undeniable change that occurred in recent years – the mainstreaming of AI. From personal use to work and education, Ireland is a country that has enthusiastically embraced the use of Generative AI tools. Official CSO data shows that about 42% of Irish internet users over 16 used tools such as ChatGPT,

Gemini or Copilot within a three-month period in 2025, compared with an EU average of roughly 33%¹. Perhaps it should be of little surprise therefore that AI use is accelerating so rapidly among Irish 8–15-year-olds. In the 3 years that we have surveyed children about their use of AI, we have seen a huge increase in engagement (Figure 26). More than half of 8–12-year-olds and over three-quarters of 12–15-year-olds are now using AI tools.

This pattern also emerges when comparing last year's focus groups – where children failed to engage with the topic of AI – with more recent sessions involving younger children (aged 9–12), who showed considerable interest in the topic. Children described regularly using AI tools such as Gemini and ChatGPT for homework, and in many cases simply to ask fun or random questions. These were also among the strongest reasons identified in our quantitative research findings (Figures 27 and 28).

The most common use is to look up information – 59% and 75% for 8–12-year olds and 12–15-year-olds respectively, which is to be expected given that AI responses are now embedded in the search engines

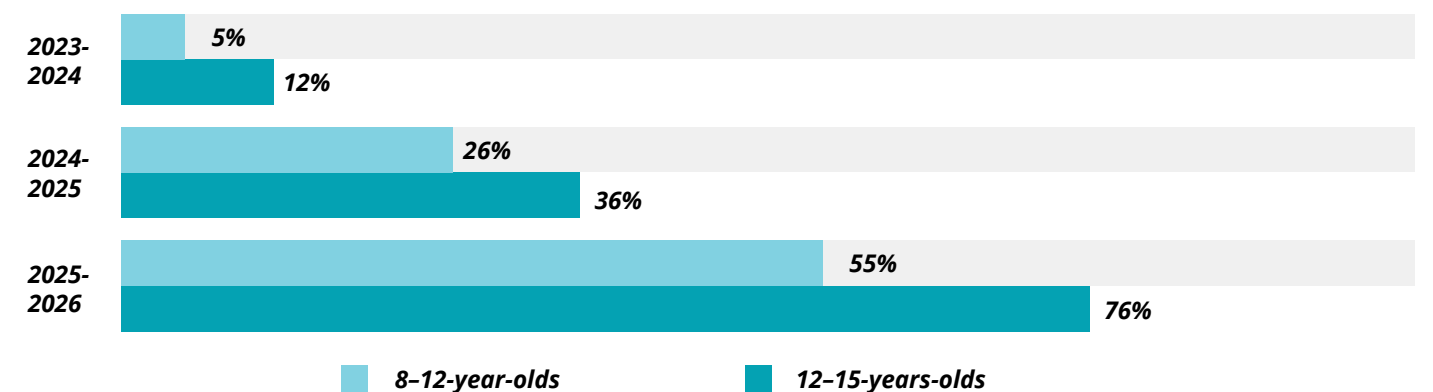


Figure 26: Adoption of AI tools, 2023–26

¹ Ref: <https://www.cso.ie/en/releasesandpublications/ep/p-isshdcb/householddigitalconsumerbehaviour2025/generativeai/>

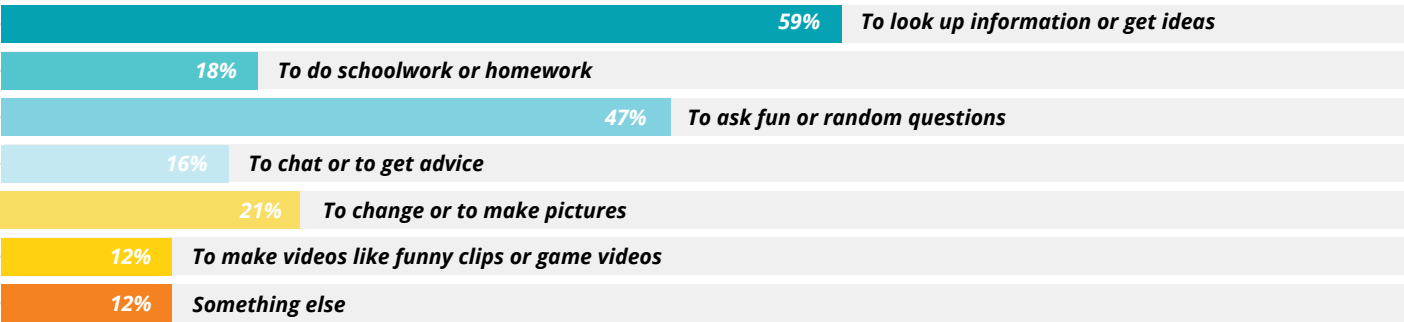


Figure 27: If you do use AI, what do you use it for? (8–12-year-olds)

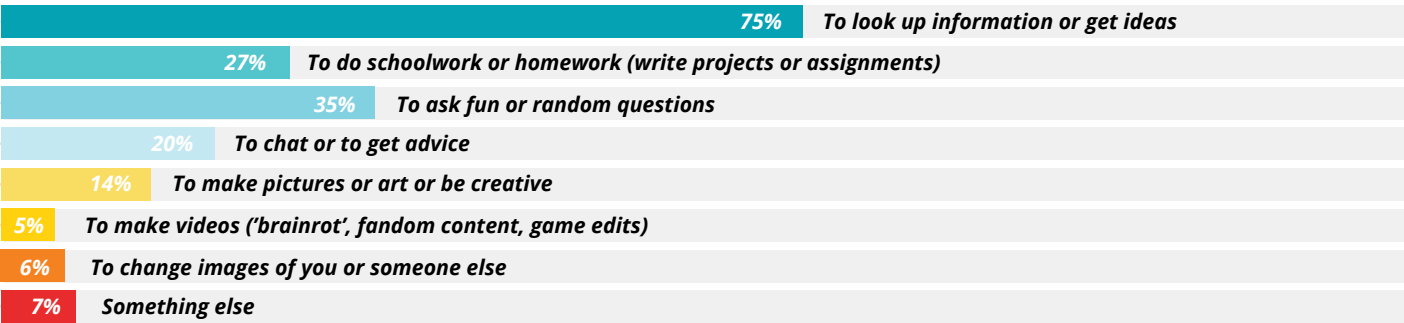


Figure 28: If you do use AI, what do you use it for? (12–15-year-olds)

that children are using, as well as being available through standalone apps.

Children's use of AI appears to evolve with age. Older respondents typically choose goal-oriented use, such as seeking information (75% of 12–15-year-olds vs. 59% of 8–12-year-olds) or support with schoolwork (27% of 12–15-year-olds vs. 18% of 8–12-year-olds). Younger children were more likely to explore AI through conversation, using it to ask imaginative, spontaneous or curiosity-driven questions (47% of 8–12-year-olds *ask fun or random questions*). The conversational design of many AI tools encourages this style of engagement.

The emphasis on entertainment is also reflected in younger children's higher use of image editing and text-to-video capabilities. 21% of 8–12-year-olds *change or make images* and 12% *make videos* (compared with 5% and 6% of 12-15-year-olds respectively).

16% of 8–12-year-olds and 20% of 12–15-year-olds use an AI chatbot *to chat or get advice*. For these young people, there may be a disconnect between viewing AI as a tool or as a friend/advisor due to the anthropomorphic design of these systems. It is well documented that social media platforms – and the AI-powered recommendation algorithms embedded within them – have been designed to capture and retain user attention. AI chatbots, however, focus on attachment, as well as engagement, and this raises new questions about emotional dependence and trust. A number of wrongful death lawsuits² are proceeding in the U.S. court system that highlight the potential for serious harm when vulnerable young people develop strong emotional attachments to AI systems.

It doesn't help that AI tools are presented as friends or advisors within apps that are already so familiar to young people. It is easy for a young person to confuse AI as a safe confidant when *MyAI* appears in a list of Snapchat friends and AI therapists are

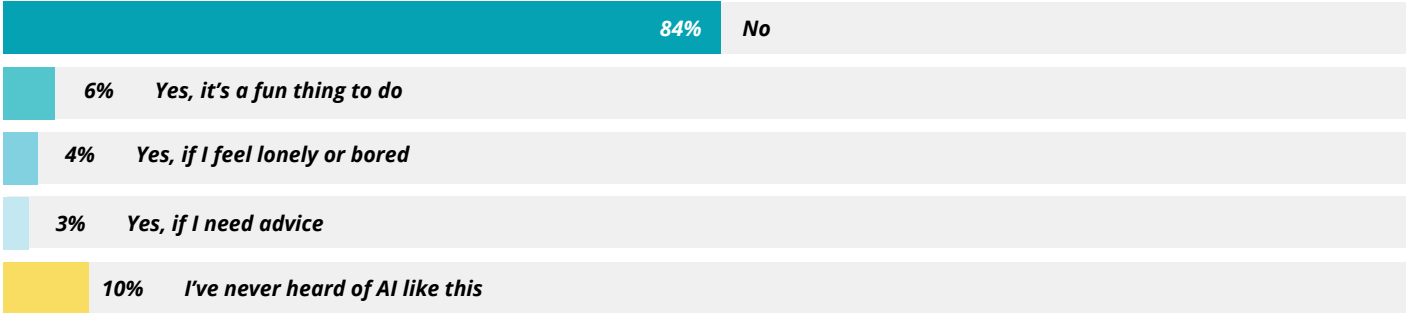


Figure 29: Do you use an app where you can talk to a character or pretend friend, like Character.AI or Replika? (8–12-year-olds)



Figure 30: Do you use an app where you can talk to a character or pretend friend, like Character.AI or Replika – or one that feels like a therapist or a boyfriend/girlfriend? (12–15-year-olds)

accessible on Roblox. In an observational study carried out by ATU Cyberpsychology students³, in consultation with CyberSafeKids, *children's avatars were exposed to explicit or disturbing mental health and trauma disclosures (e.g., suicide, self-harm, abuse, sexual assault) in AI 'therapy' experiences on Roblox*, often with no clear boundaries between role-play and real distress. These 'DIY' AI therapy bots⁴ are not regulated mental health tools, and without safeguards could amplify negative thoughts, produce harmful advice and fail to recognise a young person in crisis.

When asked specifically about their use of standalone apps i.e., *Where you can talk to a character or pretend friend, like Character.ai or Replika*, we found that younger children are more likely than older ones to engage with synthetic friends (Figures 29 and 30).

When asked for their thoughts about AI (Figures 31 and 32) only 14% of 8–12-year-olds and 16% of 12–15-year-olds say that *it gets boring after a while*, suggesting that the conversational nature of AI may make sustained interactions engaging, because these systems respond in a way that feels personal, immediate, and affirming.

It is concerning that 10% of 8–12-year-olds and 8% of 12–15-year-olds find it easier to talk to AI than to people they know in real life. A synthetic relationship may feel less challenging but at this crucial time in their social development, children learn by navigating the friction, conflict, and compromise inherent in human relationships, rather than the people-pleasing subservience of AI friends. Loneliness can be a factor in driving these interactions and it might even extend to a first-time romantic relationship for some children.

2 Ref: Raine vs OpenAI (Filed: August 2025); Garcia vs [Character.ai](#) (Filed: October 2024 / Settled: January 2026)

3 Ref: *Inappropriate Content on Roblox: An Observational Study of Exposure and Limits of Parental Controls*, Cyberpsychology Undergraduate Programme, Atlantic Technological University, 2025-2026 academic year.

4 Ref: For further information, see *When AI Therapists on Roblox Diagnose Your Child, We Have a Problem*, Substack, Sept 29th, 2025. <https://tanookialex.substack.com/p/when-ai-therapists-on-roblox-diagnose>

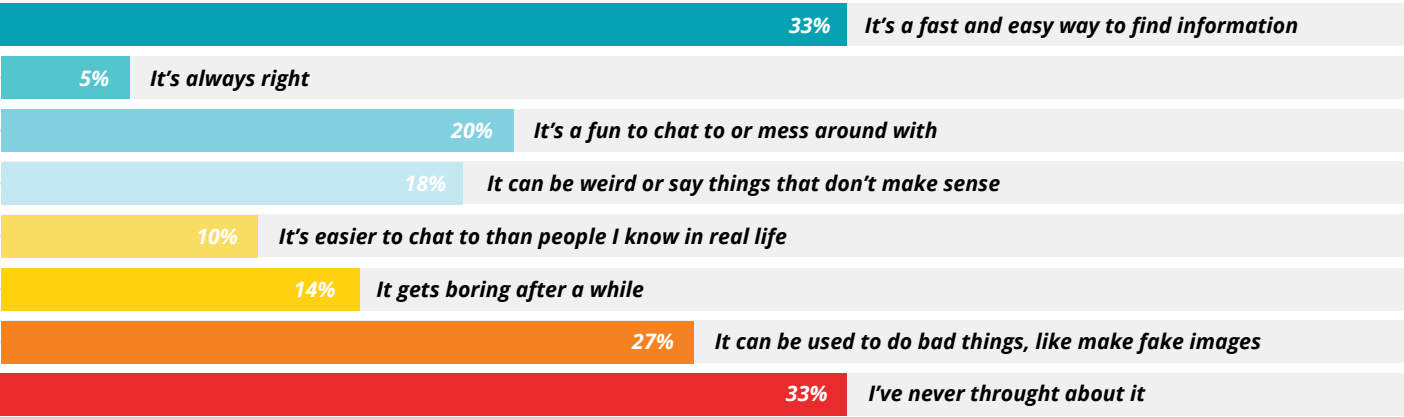


Figure 31: What do you think about AI? (8–12-year-olds)

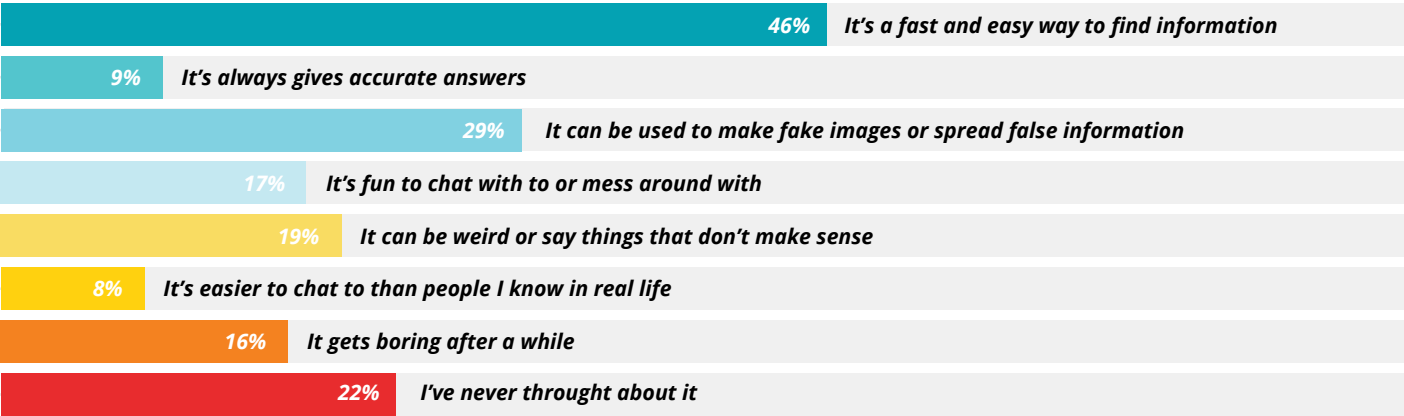


Figure 32: What do you think about AI? (12–15-year-olds)

Most young people are aware that they should not rely on the accuracy of AI responses – just 5% of 8–12-year-olds believe that AI is always right and 9% of 12–15-year-olds think the answers are always accurate. However, knowledge about AI is not evenly distributed across the children that we have surveyed (or talked with in focus groups) this year. Some children demonstrate awareness of methods used to circumvent AI facial age-estimation systems (simply drawing on a moustache according to one child) or outline strategies for spotting synthetic images, such as scrutinising details like eyes, hands, and shadows. They also spoke of encountering large volumes of what they called AI-slop, produced using tools like Sora.⁵ One 12-year-old described exposure to bot accounts sharing AI-generated fake nude imagery, while another talked about environmental

concerns. Not all children are as well-informed. In spite of well-publicised concern about AI misuse, including the creation of non-consensual intimate imagery ('nudification'), impersonation and identity fraud, and the generation of misleading or harmful content; only 27% of 8–12-year-olds know that AI can be used to do bad things, like make fake images, and 29% of 12–15-year-olds know that AI can be used to make fake images or spread false information. Sharing with AI systems can also create privacy concerns. Few children will read the terms and conditions to understand how the information that they share may be used for training the model, or shared with other third parties. Less than half – 42% of 8–12-year-olds and 41% of 12–15-year-olds – say they wouldn't share anything with AI (Figures 33 and 34).

⁵ Launched initially in December 2024, Sora was a text-to-video model developed by OpenAI. The app was shut down on April 26th, 2026 due to low user adoption, high costs and content moderation criticisms.

It is most concerning that a third of 8–12-year-olds and 28% of 12–15-year-olds have never thought about the risk of sharing information with AI. Children may spontaneously overshare when asking their fun or random questions and, more worryingly, children who turn to AI for advice may disclose highly sensitive and personal information. Feedback from focus groups and classroom discussions suggests that uploading photos of themselves and others for editing is already common practice among children. This is also reflected in quantitative findings on children's use of AI for photo editing and video creation (Figures 27 and 28), which is more common with younger children, whose understanding of privacy may be less developed.

The reason for varying degrees of knowledge about the risks and limitations of using AI is clear – many children have never received guidance from anyone about AI. Half of 8–12-year-olds and 45% of 12–15-year-olds say that no one has talked to them about using AI in a safe or smart way (Figures 35 and 36), in spite of its widespread adoption.

Only 35% of 8-12-year-olds and 32% of 12-15-year-olds have spoken to a parent about AI use. In a CyberSafeKids survey of parents, concern about children's use of AI for education, advice, and companionship ranked lowest among nine digital-related issues, with fewer than 2% of parents identifying it as their top concern.⁶ Parents may not even realise how often their children use it because AI is seamlessly embedded within everyday apps and games. Where AI has been discussed at home, children have mentioned negative comments around job losses or environmental impacts, rather than safeguarding concerns. It is also difficult for parents to offer guidance on tools that they are still trying to understand and learn about themselves.

AI is genuinely so bad for the environment... the polar bears r dying and many teachers use AI for posters or slideshows. ⁽¹³⁾

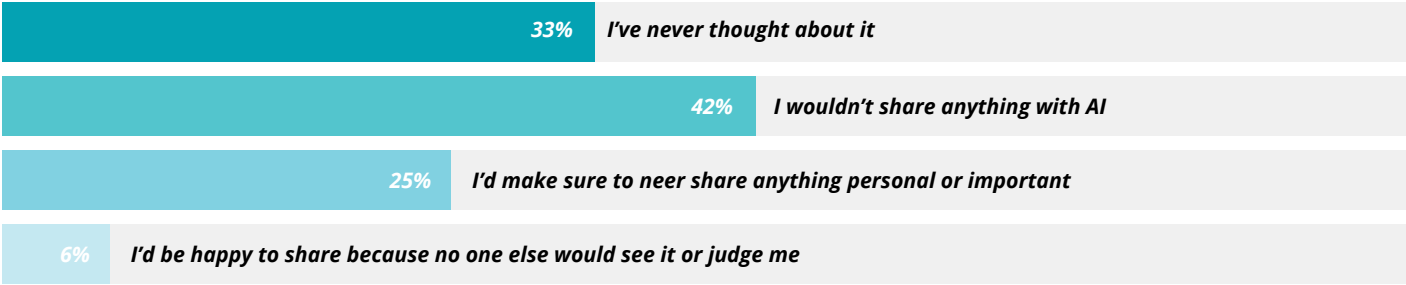


Figure 33: What do you think about sharing things with AI (like your thoughts, questions, feelings or photos)? (8–12-year-olds)

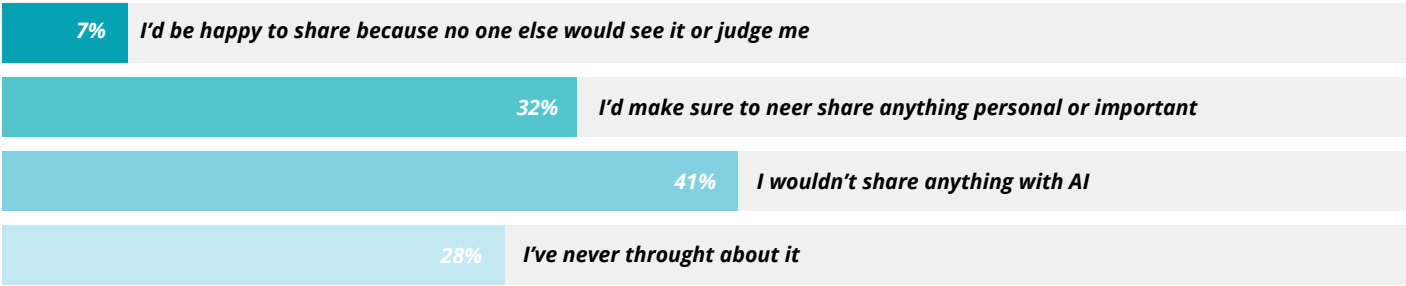


Figure 34: What do you think about sharing things with AI (like your thoughts, questions, feelings or photos)? (12–15-year-olds)

⁶ Ref: CyberSafeKids survey of over 3,000 Irish parents, 2025-2026 academic year.

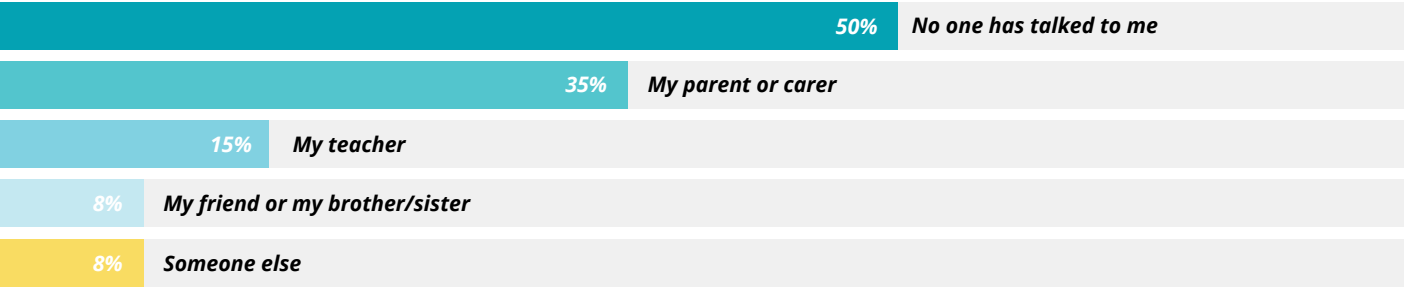


Figure 35: Has anyone talked to you about how to use AI safely and responsibly? (8–12-year-olds)

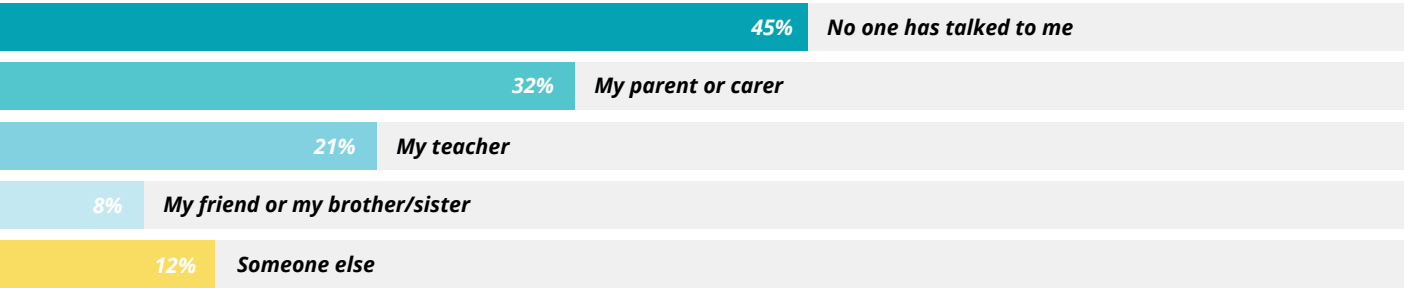


Figure 36: Has anyone talked to you about how to use AI safely and responsibly? (12–15-year-olds)

27% of 12-15-year-olds and 18% of 8–12-year-olds are using AI to do schoolwork and homework (Figure 28), a huge increase from the figures (7% and 9% respectively) reported last year: we expect this number to rise further in future years. Children have also mentioned their teachers’ use of AI for classwork, but just 15% of 8-12 -year-olds and 21% of 12-15-year-olds say that their teacher has spoken to them about using AI safely or responsibly in their own homework and schoolwork. If academic integrity is to be maintained and children are to avoid using AI as a crutch, rather than as cognitive aid, then it is essential that they are educated at school about its limitations and the need to avoid plagiarism in school and project work. Upskilling teachers with a deep understanding of AI is needed before they can successfully guide their students on its use.

It is already clear that tech companies have rushed to market with products that have not been built and assessed for children, yet children can readily access them. By embedding high-powered AI systems within apps already in use by children, adoption

and potential for harm has happened at a terrifying speed. A prime example is the controversial introduction of Grok on X. So-called ‘nudification’ capabilities weren't new, but they suddenly went mainstream because the higher barrier to entry was erased and awareness increased. Reacting to public criticism, tightening EU regulations, and legal pressures in the US, tech companies have shifted their official terms to require users to be at least 13 (with parental consent) or 18, and introduced age assurance guardrails (including behavioural scanning and biometric verification if flagged). Parental controls were added to ChatGPT and WhatsApp has added parent-managed accounts, which don’t include Meta AI. This all feels reminiscent of other failed child protection approaches adopted by social media companies, rather than focusing on safety by design. Meanwhile, children themselves do not report finding it difficult to access AI systems as either standalone platforms or embedded in apps familiar to them: we have already noted the failures in age assurance (see section *Age Not Assured*) in the latter. When our attention is focused on the mental health impacts of social media use, these untested

AI products are already in the hands of children, and as one 11-year-old said, 'AI is going to be in our future'.

Regulation of AI in the EU lags behind the technology it seeks to govern, with implementation deadlines slipping further into 2027 and 2028. However, if we don’t prioritise child safety in AI development today, we are doomed to repeat the reactive approach taken with social media, where action comes way too late and only after significant harm has emerged.

A Note on Regulation: the EU’s AI Act began a phased application from 2024. Transparency and high-risk obligations (including those most relevant to vulnerable groups including children, such as AI used in education) were due to take effect from August 2026 but the Digital Omnibus on AI – agreed in May 2026 – delayed these obligations to December 2027 and August 2028.



United And Divided

Please do not ban under 16 years because it needs to be safer and people need to be smarter when going, and you adults have to help us. ⁽¹⁰⁾

We have tablets but I'm only allowed to use it when my mom says I can and its for a set time. I look at YouTube sometimes but I'm only allowed to watch kids tube unless my mom or dad are showing me something on normal YouTube. ⁽⁹⁾

Even before questions of AI or the influence of algorithms, there is a simpler gatekeeper to a child's digital life: the smart device that enables it. We have seen some significant changes with regard to who has one (and when they receive it) in recent years, although those changes have not been universal.

Smart device ownership among 8–12-year-olds in Ireland remains high this year at 94% (Figure 37). Tablets and games consoles are firm favourites, with ownership rates of 63% and 57% respectively. As always, there are significant differences between boys and girls regarding their choice of devices, with gaming consoles far more popular with boys (81% vs. 32%) and tablets with girls (69% vs. 56%) (Figure 38).

Reflecting the type of games they favour, boys are also more likely to own VR headsets and computers than girls.

Delaying the purchase of smartphones has been the focal point for collective, parent-led movements in recent years.¹ While identical apps and games are often accessed from other smart devices, the portable nature of the smartphone makes it harder for parents to monitor and for children to get a psychological break, so it is widely recognised as the most challenging smart device for a young person to own. Last year we reported a significant decline from 49% ownership among 8–12-year-olds in 2023–2024, to 39% in 2025–2026, crediting grassroots, 'hold off' movements. Following the drop last year, ownership has largely stabilised at 36% this year.²

Smartwatches and minimalist phones have been adopted in some households as alternatives. 1% of 8–12-year-olds own a phone that has *limited functionality and access to apps* and smartwatches are far more popular this year than last (30% ownership, up from 22%). Most smartwatches owned by this age group come *without internet and apps like an Xplora, Fitbit Ace LTE* (24% vs. the 6% who own a fully connected smartwatch). They offer families a way to keep in touch without providing a fully functional, portable smart device.

Collective, parent-led movements have also tried to delay children's uptake of 13+ social media apps in recent years, with some success. The peak surge in social media activity for 8–12-year-olds occurred in 2021–2022, when children were forced online for entertainment and socialisation during the pandemic and resulting school closures. That

¹ Pioneered by Greystone's 'It Takes a Village' initiative, supported by Smartphone-Free Childhood Ireland, <https://smartphonefree.ie/>.

² A 3% difference is within normal sampling variation and is not considered statistically significant.

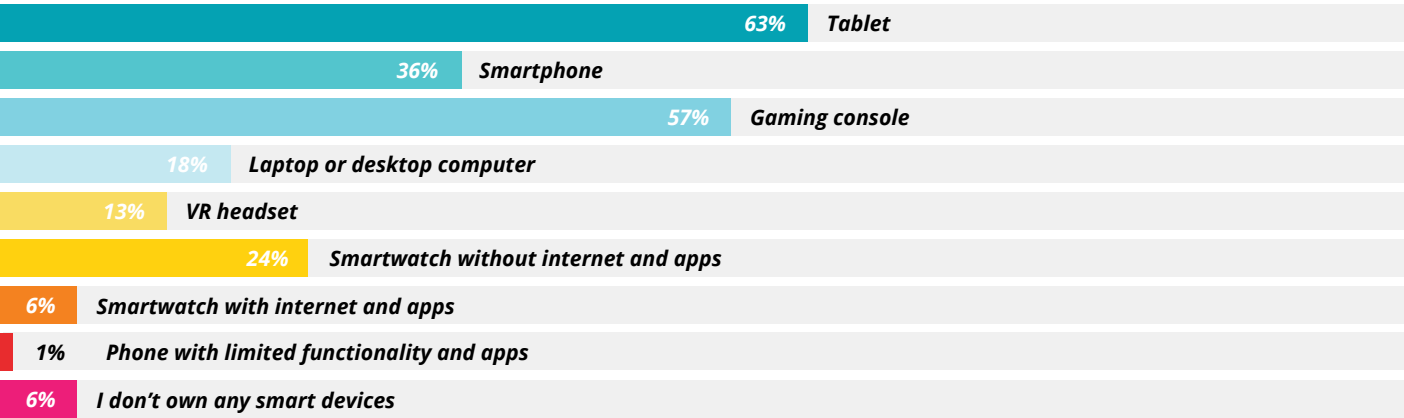


Figure 37: Which smart devices do you own yourself? (Tick any that belong to you, not devices your parents own and let you use sometimes) (8–12-year-olds)

year, 47% had accounts on TikTok and 40% on Snapchat. But even before the pandemic, usage of apps including TikTok and Snapchat was much higher than it is today because parents were less aware of risks and harms – 40% had accounts on TikTok in 2019-2020 and 34% on Snapchat. Parents working together to delay uptake of certain social media apps has resulted in the much lower levels we observe today – this year 21% and 20% of 8–12-year-olds respectively have accounts on Snapchat and TikTok. We credit parents for this lower level of usage, as the most significant drop occurred last year before any regulatory changes, followed by only a marginal decline this year that falls within the range attributable to sample variation: Snapchat (21%) is down from 25% last year, and TikTok (20%) is down from 23%.

However, we need to be wary of the alternatives young children are adopting for online entertainment and connectivity. Reduced smartphone ownership and social media use risks giving parents a false sense of security if children simply pivot to other social apps, games, and smart devices. Connecting through tablets, consoles, laptops and VR headsets remains widespread and Roblox is more popular than ever, a platform that can expose children to many contact and content risks (see section *Growing Up On Roblox*). Parents can also be less concerned

about YouTube usage, due to their own familiarity and its widespread educational use, but a significant number of children (26% of 8–12-year-olds) report negative experiences on the platform (see section *When Safeguards Fail*).

It is heartening to see that parents, by working together, have reduced peer pressure on younger children and successfully changed the online access norms in some communities. These new norms are not universally felt however, and tend to be concentrated in highly resourced and more populated areas. As a result, the digital safety of 8–12-year-olds today still too often depends on their postcode.

In disadvantaged communities, there can be complex and systemic challenges faced by families, from economic insecurity to digital literacy and language barriers, which mean that overextended families are not in a position to act collectively. It is also important to recognise that children's online engagement is shaped by the opportunities available offline. In communities with fewer safe public spaces, recreational facilities, or affordable organised activities, online environments may play a greater role in enabling young people to socialise.³

³ We explore this resulting digital inequity further in the section *Safety Online: A Right or Privilege?* below.

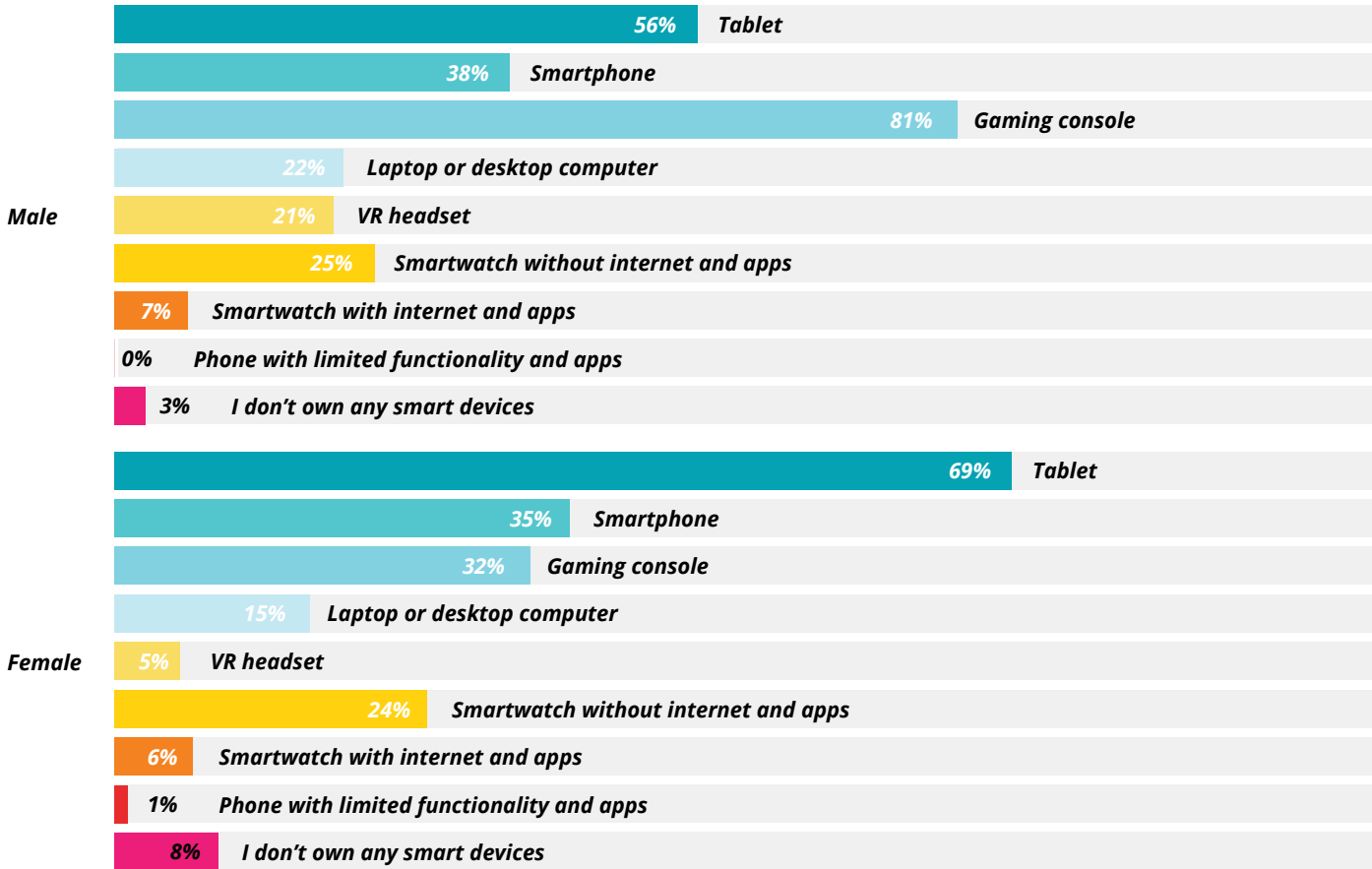


Figure 38: Which smart devices do you own yourself? (By gender, 8–12-year-olds)

Most collective movements are also found in major population centres. Geographical and logistical barriers can impact the feasibility of collective parenting agreements in some areas of the country. It can be more difficult for children to meet peers in person in rural areas, so accessing digital spaces may be viewed as essential for socialisation. Additionally, children who are bused to school may be given a phone primarily for practical safety purposes.

Access among 12–15-year-olds is also unlikely to drop if doing so relies solely on a coordinated and sustained effort from parents. Older children are more likely to travel independently to post-primary schools, often farther afield, and their parents are less likely to have direct or regular contact with the parents of their friends. As a result, collective parental action is more challenging to organise when children move to post-primary education, and getting a smartphone remains something of a

'rite of passage'. There is a substantial increase in smartphone ownership among 12-year-olds from 54% in primary schools to 92% in post-primary schools.

Smart device ownership among 12–15-year-olds remains high at 99%, with 93% owning a smartphone and many owning multiple devices (Figure 39). Some families are choosing alternatives to the fully functioning smartphone. 4% of 12–15-year-olds this year *own a phone that only does basic things, with very few apps, like a Balance phone*. Smartwatches are less popular with 12–15-year-olds than younger children, but they are more likely to *own a watch with internet and apps, such as an Apple Watch* (13% of 12–15-year-olds vs. 6% of 8–12-year-olds). There continues to be significant differences between genders in this age group. Girls of 12–15-years are more likely to own a smartphone (95% vs. 91%) or a tablet (55% vs. 36%), while boys are more likely to own a gaming console

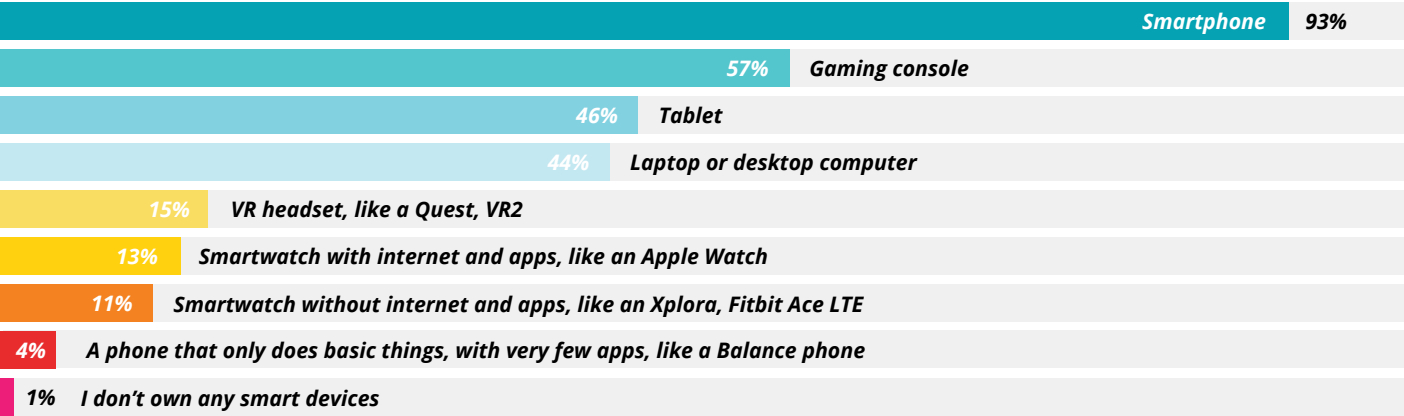


Figure 39: Which smart devices do you own yourself? (Tick any that belong to you, not devices your parents own and let you use sometimes) (12–15-year-olds)

(79% vs. 33%). The higher prevalence of laptop and desktop computer ownership among older children (44% vs. 14% for 8–12-year-olds) reflects the greater educational demands associated with post-primary education, where these devices are increasingly used for schoolwork.

I don't like being online but I get fomo if I'm not. (14)

I feel like it is too addicting and it's hard to stop. (11)

Across both age groups, the need to fix the digital environment itself does not go away by placing the burden of creating solutions on parents alone, whose circumstances may be vastly different. Even in areas where collective action has been very successful, delaying access is only part of the solution. Children have a right to digital access under

the UN Convention on the Rights of the Child⁴, and for some – including those who are neurodivergent, isolated, or from marginalised communities – these digital environments can be a vital outlet once access begins. Delay buys time but it is not a substitute for safe design, defined as age assurance, safer defaults, and algorithms that serve wellbeing over engagement. This year, almost half of children (49% of 8–12-year-olds and 51% of 12–15-year-olds) feel they spend too much time online, a consequence of platforms designed to maximise engagement. True digital protection means the safety of a child online is guaranteed by design and law, not determined solely by their parents' capacity to shield them from systemic digital harms, nor on keeping them offline altogether.

⁴ Ref: <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>

Safety Online: A Right or Privilege?

To further understand how localised socio-economic factors influence children's access, the research data¹ has been disaggregated using the Department of Education's DEIS (Delivering Equality of Opportunity in Schools) model.

Ownership levels for a smart device among 8–12-year-olds is similar across both DEIS-designated and non-DEIS schools (96% and 94% respectively). In DEIS schools, however, smartphones are the most

popular device, with a staggering 62% of 8–12-year olds owning a fully functional smartphone, more than twice the level observed in non-DEIS schools (29%).

The huge decline that we have observed in smartphone ownership in non-DEIS schools over the past two years, attributed to collective parental action, has not been replicated in DEIS schools. Ownership levels here have remained almost the same (from 65% to 62%), compared with a large decline (from 43% to 29%) in non-DEIS schools.*

DEIS-designated	Non-DEIS
62% Smartphone ownership	29% Smartphone ownership
83% Have accounts on 13+ regulated social media app(s)	66% Have accounts on 13+ regulated social media app(s)
34% Play 18+ games	18% Play 18+ games
35% TikTok	15% TikTok
35% Snapchat	17% Snapchat
73% YouTube	60% YouTube
50% WhatsApp	24% WhatsApp
78% Roblox	65% Roblox
47% Go online whenever they want	26% Go online whenever they want
91% Access devices in bedrooms	75% Access devices in bedrooms
32% Bothered by harmful contact/content online	24% Bothered by harmful contact/content online
36% Cyberbullied	26% Cyberbullied

*Comparative statistics are from academic year 2023–24

¹ Survey sample of 8–12-year-old pupils in primary schools this academic year: 1,363 from 15 DEIS schools and 4,685 from 43 non-DEIS schools.

Access to the most popular 13+ apps (YouTube, WhatsApp, Snapchat, and TikTok) is significantly higher among pupils in DEIS schools, and a much higher proportion of 8–12-year-olds in DEIS schools play 18+ games, with close to half of boys doing so (46%). This gap exists for Roblox and YouTube also, but as mentioned previously, concern among parents in general regarding these platforms is lower so the gap is smaller.

We have not observed a significant difference in access for 12–15-year-olds attending DEIS and non-DEIS schools. This is not surprising, as the logistical reasons previously discussed make collective arrangements harder to sustain for parents of older children, and parents across all communities are less involved in their children's digital lives when they move into post-primary education.

DEIS pupils of 8–12-years are also much more likely to be able to operate online without time restrictions (47% DEIS vs. 26% non-DEIS) and to have access to personal devices (quite likely a smartphone) in their bedrooms (91% DEIS vs. 75% non-DEIS), even overnight (69% DEIS vs. 50% non-DEIS).

Despite similar AI adoption rates by 8–12-year-olds across all communities (57% DEIS vs. 54% non-DEIS), a gap exists in active parent-child discussions on this topic (29% DEIS vs. 37% non-DEIS), underscoring the importance of providing accessible, community-wide AI literacy initiatives, as well as school-led guidance for children.

Children in DEIS schools are more likely to be exposed to something that bothered them online (32% DEIS vs. 24% non-DEIS) and to experience cyberbullying (36% DEIS vs. 26% non-DEIS). This is unsurprising given they may be spending more time online and in environments that were not designed for them. It is still possible that children in DEIS schools are under-reporting negative experiences because repeated exposure can raise the threshold for what a child perceives as shocking or concerning, a pattern reflected in testimonials received from children in different communities.

It is clear from our findings that collective, parent-led action can be effective in delaying access and reducing harm but while parental concern for child safety is universal, collective action is harder to organise and sustain in disadvantaged communities.

Families' socioeconomic resources are too varied to treat child safety online as a private parenting obligation. To address digital inequity, safety-by-design principles and systemic interventions are needed, alongside school-led educational supports. It is also necessary to address the physical environment, providing more offline alternatives to young people in more disadvantaged communities.



Our Recommendations

CyberSafeKids calls for:

- 1** Implementing Ireland's Online Health Taskforce recommendations without delay.
- 2** The European Parliament and Council to agree on EU-level prohibitions on the marketing and use of AI systems for the creation of non-consensual intimate images.
- 3** Blocking minors' access to pornography in Ireland, as required under the Digital Services Act's Article 28 guidelines.
- 4** Government and civil society-led initiatives to support and inform parents and caregivers.
- 5** An amendment to the Digital Services Act (or new legislation) setting 16 as the default minimum age for digital products intended for use by children – a presumption platforms can circumvent only where they can demonstrate, through pre-certification from an independent classification board, that a lower age rating is appropriate.

Against a backdrop of significant growth in the tech industry's AI capabilities, and with the new knowledge that children's use of AI is growing exponentially annually, the 'move fast and break things' ethos that defined social media and online gaming is being replicated once again. With the same disregard from industry, and arguably regulators, for fundamental safeguards and the most vulnerable users, the consequences cannot be overstated.

China's *Interim Measures for AI Anthropomorphic Interaction Services* took effect on 15th July 2026, targeting addiction and self-harm in services like chatbots and virtual companions. Virtual companion services are now banned outright for all under-18s, with parental consent required for other such services for under-14s. Europe's approach seems to run in the opposite direction. Rather than tightening obligations for high-risk AI, the *Digital Omnibus on AI* – agreed in May 2026 – pushes those obligations back to December 2027 and August 2028. Many observers see this as a weakening of protections that were insubstantial to begin with.

Elsewhere, Australia's under-16 social media ban has been in force since December 2025, with Malaysia,

Indonesia and New Zealand, in addition to a number of European countries, now moving to follow. And on 13th July 2026, the European Commission's own *Special Panel of Experts*, in which CyberSafeKids took part, recommended a framework requiring platforms to prove their services are safe before they reach children. We hope that legislation, expected to follow the publication of the report, will make this pre-market access requirement a reality.

The more we observe this landscape – children's online experiences, fearful, overwhelmed and overstretched parents, policymakers struggling to keep pace, the challenges regulators face enforcing the law – the more strongly we conclude that the current model is failing children. Why is every other product intended for a child, such as food, medicine or toys, subject to rigorous compliance testing before it reaches them, while Big Tech gets a free pass? The current system requires harm to be proven *after the fact*, and even then faces endless legal challenges. It should work in reverse: platforms should not be allowed to access the child market unless they can first prove their products are safe.

Our recommendations are as follows:

1

We urge the Irish Government to implement the Online Health Taskforce recommendations without delay. This should include the fifth recommendation from their report: an evidence-informed critical digital literacy campaign and education programme delivered nationwide. Children's engagement with digital environments is routinely described by senior government officials as a 'public health crisis', yet no considered public health response has followed.

2

We call for the European Parliament and Council to agree on EU-level prohibitions, under the AI Act/Digital Omnibus amendments, on the marketing and use of AI systems for the creation of non-consensual intimate images. This must cover both provider/distribution and deployer use. We call for this prohibition to be applied broadly enough to capture partial as well as full 'undressing' – including edits to swimwear or similar minimal clothing – rather than being narrowly read as covering only intimate parts or sexualised imagery. At national level, Ireland must ensure equivalent enforcement.

3

We call for urgent action by the Irish Government to block minors' access to pornography, as already required under the Digital Services Act's Article 28 guidelines. Providers of adult content are required to implement trusted third-party age verification – not age assurance, inference, or estimation – and the government must urgently set out how this will be fully realised in the Irish context.

4

We call for Government and civil-society-led initiatives to support and inform parents and caregivers. Digital parenting and caregiving is now an integral part of raising children, and the same protective standards that apply offline must also apply online.

5

An amendment to the Digital Services Act (or new legislation) setting 16 as the default minimum age for digital products intended for use by children – a presumption platforms can circumvent only where they can demonstrate, through pre-certification from an independent classification board, that a lower age rating is appropriate. These measures should apply to all products potentially used by children, unless platforms can prove they're appropriate for younger ages, with pre-certification issued by an independent classification board. Lowest age-ratings should require, at a minimum, no engagement-maximising design (e.g. autoplay, infinite scroll), no behavioural profiling, no randomised monetisation mechanics (e.g. lootboxes), and tight restrictions on AI companion features. As with all other products meant for children, the precautionary principle should inform the approach, and certification should be time-bound and subject to regular review. Failing EU-level movement, we must see standalone Irish child safety legislation.





Children's Digital Lives in Ireland, 2025–26



Deloitte.