



Children's circumvention behaviours online

Full report

July 2026



Department for
Science, Innovation
& Technology

Table of contents

Background & Research Objectives 4

Methodology 6

Executive Summary 7

Section 1: VPN users, motivations and facilitation 10

Section 2: Encountering age checks 26

Section 3: Bypassing age checks 31

Section 4: Harms faced online 44

List of Figures

Figure 1:	VPN awareness and use by age group	11
Figure 2:	Frequency of use among VPN users	12
Figure 3:	When did children start using VPNs?	13
Figure 4:	Devices children use VPNs on	14
Figure 5:	Reasons for VPN use	15
Figure 6:	Perceived importance of online privacy	17
Figure 7:	How children define online “Privacy”	18
Figure 8:	The extent to which VPNs make children feel safer online	19
Figure 9:	Help received to set up the VPN.....	20
Figure 10:	Who helps set up VPNs?.....	21
Figure 11:	Help with setting up VPNs by age group.....	23
Figure 12:	Who pays for the VPN?	24
Figure 13:	Method of paying for VPN by age	25
Figure 14:	Age checks encountered	26
Figure 15:	Encountering of advanced checks by age	27
Figure 16:	Perceived efficacy of age check types	28
Figure 17:	Perceived purpose of age checks.....	29
Figure 18:	Trust in age checks	30
Figure 19:	Age check circumvention by age	31
Figure 20:	Reasons for avoiding age checks or findings easy age checks	32
Figure 21:	Success of bypassing age checks	33
Figure 22:	Methods of bypassing age checks	35
Figure 23:	Reasons for bypassing age checks	37
Figure 24:	Perceived ease of bypass methods	38
Figure 25:	How children learn to bypass age checks	39
Figure 26:	Bypassing success by set up of VPN	40
Figure 27:	Parental awareness of bypassing success	41
Figure 28:	Perceived risks of bypassing age checks	42
Figure 29:	Deterrents of bypassing age checks.....	43
Figure 30:	How harmful content was experienced	45
Figure 31:	Content most likely to be seen after bypassing an age check.....	47
Figure 32:	Recent experience of harmful content online in all children and VPN users.....	48

Background & Research Objectives

In July 2025 the Online Safety Act's child safety duties came into force, requiring in scope services to use highly effective age assurance to stop children seeing the most harmful types of content online. Alongside the introduction of these protections, questions were raised about whether some children might seek ways to get around them. This sits alongside a wider public debate about whether access to some online services should be restricted to children altogether, and how effective such restrictions would be.

The Department for Science, Innovation and Technology (DSIT) commissioned BMG Research to build a robust evidence base on how children aged 11 to 17 experience age assurance, whether and why some seek to get around it, and the role that virtual private networks (VPNs) and other tools may play. The findings are intended to support DSIT and Ofcom's understanding of children's experiences of age assurance, circumvention and VPN use, and to inform future policy development in this area.

Research objectives

The research set out to answer three core questions:

- How are children experiencing age assurance checks online, and how effective do they think they are?
- What are the most common ways children get around age checks, and why?
- What motivates children to use VPNs, and how do they access them in practice?

Throughout the report, findings are examined across key groups of interest: age (11 to 12, 13 to 15 and 16 to 17), gender, VPN users, children who spend a lot of time online, children with a special educational need or a limiting condition, and children in financially vulnerable households.

Policy Context

The Online Safety Act places duties on a wide range of online services. Its child safety duties, in force since July 2025, require services that are likely to be accessed by children to use highly effective age assurance to prevent children from encountering content that is harmful to them. In June 2026, the government also announced its intention to introduce measures preventing social media platforms from offering their services to under-16s.¹

Following the implementation of age assurance requirements, there has been public and Parliamentary interest in whether users are circumventing age checks. VPNs are one tool that can alter a user's real location online and be used to evade age assurance measures. Ofcom reported that daily active users of VPN apps in the UK temporarily doubled to around 1.5 million following the introduction of the child safety duties, before falling back to 900,000 by November.² However, it was not clear whether this spike was driven by children or adults seeking to avoid age checks.

Understanding the prevalence of VPN use among children, their reasons for using VPNs, and how this relates to circumvention is therefore important for developing robust and evidence-based

¹ [Government announcement for social media ban for under-16s](#)

² [Ofcom: Online Safety in 2025](#)



policy. This evidence also supports the government's wider work on children's online experiences, including the Growing up in the Online World consultation.

Age checks

Throughout this report, the term 'advanced age checks' or 'advanced age assurance' refers to age assurance methods such as facial age estimation, government ID verification, payment card verification and third-party age verification services. These methods are commonly associated with **highly effective age assurance**, as described in Ofcom's guidance.

Services in scope of the Online Safety Act's child safety duties are required to use highly effective age assurance to prevent children from encountering harmful content. Self-declaration methods are not considered highly effective, whereas methods such as facial age estimation and government ID checks are.

Interpreting these findings

Evidence presented in this report relies on self-reported behaviours from both parents and children. As with any self-reported data, there may be reasons why some behaviours are over- or under-reported. Some measures also use wording around "settings or tools" that change a child's apparent location rather than referring to VPNs directly, so that children who had not done this were not inadvertently shown how to do so.



Methodology

Questionnaire development

The questionnaire was developed by BMG Research and the Department for Science, Innovation and Technology (DSIT). Prior to launch, the survey link was cognitively tested with 10 children and their parents. Questionnaire updates were informed by cognitive testing.

Sample and approach

A total of 2,299 young people aged 11 to 17 completed the survey, with a nationally representative sample of 2,029 sampled alongside a boost of 270 of those who had used a VPN in the last three months.

The sample is nationally representative by age, gender, country and socioeconomic group. The VPN user boost respondents were added into the nationally representative sample and weighted to match the nationally representative incidence of VPN usage in the past 3 months.

The survey was set up to be asked of parents/guardians initially before passing the device to their child. For those aged 16 to 17, a sample was drawn from those who answered after being passed the survey by their parents (568) and those who answered the survey directly (217).

Data was collected using a blend of online panels from the 18th of May 2026 to the 29th of May 2026.

Quotas were set in line with nationally representative fallout by nation, region, child age by gender, socioeconomic grade, Index of Multiple Deprivation quartiles, and rurality.

Weighting and analysis

Data was weighted to be representative of UK children aged 11 to 17.

Unless stated otherwise, all percentages are based on weighted data. Differences described as higher or lower in the text are statistically significant at the 95% confidence level.



Executive Summary

VPN use

- **Around a quarter of children use a VPN, and use rises sharply with age.** Nearly six in ten (58%) have heard of VPNs. A quarter (26%) say they have used one in their lifetime and around a fifth (22%) have used one in the last three months. Lifetime use rises from 17% of 11- to 12-year-olds to 31% of 16- to 17-year-olds.
- **Among children who have used a VPN, use is frequent.** Around two-thirds (64%) use one at least weekly.
- **Children's reasons for using a VPN are focused on privacy and content.** The most common reasons are to keep their activity private (30%), to access certain websites, apps or games (27%) and to watch videos from other countries (25%). Around a fifth of VPN users (22%) say they use one specifically to reach age-restricted websites, apps or games, which equates to 7% of all children saying they use a VPN to reach age-restricted websites, apps or games.
- **Most children who use a VPN feel safer for doing so, and value their privacy highly.** Eight in ten VPN users (81%) say it makes them feel safer online. Privacy matters to 86% of all children, rising to 90% among lifetime VPN users and falling to 84% in non-VPN users.
- **Parents are often involved in children's VPN use.** Of those who have used a VPN in their lifetime, 22% had been helped by a parent to set it up, and 43% of child VPN users say a parent pays for it, while 36% say their VPN is free.

Encountering age checks

- **Most children (78%) have encountered some form of age check.** Around one in five (19%) children aged 11 to 17 say they have never come across one.
- **The checks children meet most often are the simplest.** Over half of all children have encountered a tick box (57%) or been asked to enter their date of birth (56%). A minority (45%) have encountered any of the more advanced checks associated with the Online Safety Act: facial age estimation (26%), uploading a government ID (17%), payment card verification (17%) and third-party identification apps (14%).
- **Children rate the more advanced checks as the most effective.** Government ID upload is seen as effective by 86% of children who have come across this check, payment card verification by 74% and facial age estimation by 73%. By contrast, a majority (54%) of those who have come across tick box age checks think it is not effective. The two checks the majority of children have met (ticking a box or providing a date of birth) are also the two they least believe work.

Bypassing age checks

- **Over half of children choose platforms to avoid age checks altogether.** 53% of all children say they have deliberately picked a website, app or game to sidestep a check: 37% because it had no age check, and 34% because the check would be easy to get around.



- **Nearly two in five of all children have also successfully got around a check directly.** This includes both advanced checks and simpler checks like tick boxes and entering a birth date. 39% of 11- to 17-year-olds say they have got around an age check at least once, and a further 14% have tried without success (53% in total have attempted it). Success rises from 28% of 11- to 12-year-olds to 43% of older children and is much higher among children who have used a VPN (56%, against 33% of those who have never used one) and particularly children who set up a VPN themselves (71%), an association that cannot be fully explained by the older age skew of VPN users.
- **Pretending to be older is the most common method.** Around two-thirds (63%) of children who say they have bypassed a check do so by posing as someone else (this amounts to 24% of all children).
- **10% of all children say they have bypassed age checks by using settings or tools that change their apparent location.** Among those who have bypassed age checks, 27% say they have used settings or tools that change their apparent location. This equates to 10% of all children.³ Most who try find it easy: 71% of children who say they have pretended to be someone else to bypass age checks found getting around them using that method easy, while 64% of children who say they have used settings or tools to change their location found it easy.
- **Most reported circumvention relates to self-declaration checks rather than advanced age assurance.** Children who have bypassed an age check are most likely to have encountered self-declaration checks (73% a tick box, 71% asked to provide their date of birth). The most commonly cited way of pretending to be old enough to get around an age check was giving a false date of birth (45%). Around six in ten of those who bypassed (60%) have also encountered at least one advanced check, such as facial age estimation (37%) or government ID upload (24%). 11% of those who pretended to be someone old enough to get around an age check said they used a parent's or relative's ID, while a lower proportion had used someone else's ID (5%) or used altered images or disguises to appear older (6%), but these were in the minority.
- **Children most often learn how to bypass an age check from friends their age (50%).** Around a fifth of children who have bypassed have worked it out themselves (21%) and 10% have learned from a parent or guardian. Awareness of the risks⁴ is high but does not appear to deter them: only 6% of those who have got around a check say none of the potential risks would apply to them.
- **The deterrents children rate most highly are practical ones.** Age checks that are harder to get around (44%), the threat of an account being permanently banned (40%) and parents being notified if they try (39%) are all selected as deterrents by a large majority of children who have bypassed age checks.

Harms faced online

- **A notable share of teenagers both use a VPN and have encountered explicit material in the same period.** In the last three months, 16% of 13- to 17-year-olds say they have

³ This wording was deliberately chosen as a proxy for VPN use, so that children who had used a VPN but not for bypassing age checks were not directed toward how to do so.

⁴ Risks included: seeing upsetting content, talking to strangers, sharing information that put them in danger, downloading harmful apps/software, exposure to scams and sharing location without realising it.



seen explicit sexual content or nudity online. 7% of 13- to 17-year-olds have used a VPN in the last three months and seen explicit sexual content.

- **Most harmful content children encountered in the prior three months is encountered passively while scrolling, rather than searched for.** This includes explicit sexual content where 40% of those who encountered it were scrolling, compared with 25% who were actively searching for it.
- **Many are encountering harmful content after bypassing.** Among children who bypassed age checks, 51% said they had encountered at least one type of harmful content after bypassing checks (20% of all children). Looking at specific types, among those who have bypassed checks, explicit sexual content was most likely to be only seen after bypassing checks, with 35% of those who had bypassed and seen it in the last three months saying they had done so only after getting round an age check, followed by contact from unknown adults (29%) and requests for personal information (27%). VPN users who bypass have a particularly high association with seeing harmful content: 64% of children who used a VPN in their lifetime saw harmful content after bypassing, compared with 43% of those who bypassed but have not used a VPN in their lifetime. Although there are some age effects behind the proportion of VPN users reporting this, this cannot explain the full extent of the results.



Section 1: VPN users, motivations and facilitation

Over half of children are aware of VPNs

As part of a series of questions exploring children's awareness and use of VPNs, we asked 11- to 17-year-olds if they had ever heard of VPNs, used VPNs in their lifetime, or used a VPN in the past 3 months.

Awareness of VPNs is widespread. Nearly six in ten (58%) children aged 11 to 17 say they have heard of VPNs. Boys are more likely to have heard of VPNs than girls (63% vs. 53%), while children aged 13 to 15 (61%) or 16 to 17 (70%) are more likely than those aged 11 to 12 (41%).

A quarter of children have used a VPN in their lifetime

Awareness does not translate directly into use. Around a quarter of children (26%) say they have used a VPN in their lifetime. This is just under half (45%) of children who are aware of VPNs in the first place. Fewer than one in five 11- to 12-year-olds (17%) have used a VPN in their lifetime. This rises to nearly three in ten (29%) 13- to 15-year-olds and just under a third (31%) of 16- to 17-year-olds.

Use varies across demographic groups.

- Children in London are notably more likely to have used a VPN than elsewhere, with two in five (37%) reporting lifetime use, well above the national average.
- Socioeconomic background plays a role too. Children from higher socioeconomic households (ABC1) are more likely to have used a VPN (31%) than those from C2DE households (20%).
- Children from ethnic minority backgrounds are also more likely to report VPN use (30%) compared to white children (25%).
- Children in households of 2 to 3 children are more likely to report use of a VPN (28%) than those in single child households (23% usage), highlighting the role of siblings in VPN adoption. In fact, 8% of children who had help setting up a VPN were assisted by a sibling.

Around one in five children have used a VPN in the last three months

Over a fifth (22%) of children report having used a VPN in the past three months. Children aged 13 to 15 (26%) and 16 to 17 (25%) are significantly more likely than those aged 11 to 12 (14%) to have done so.

The proportion of children who have ever used a VPN is close to the proportion who continue to use them, with 22% saying they have used in the last three months, compared with the proportion who report ever using one (26%).

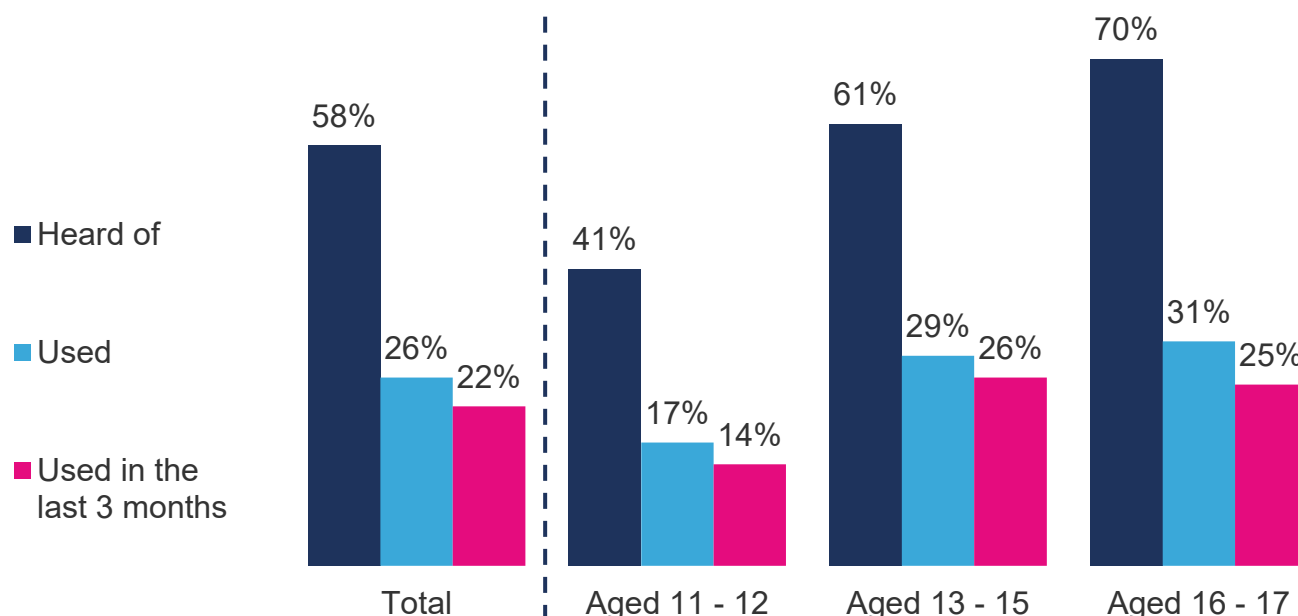
These findings sit broadly in line with other recent research in this area. In March 2026, Ofcom reported that 29% of 11- to 17-year-olds have used a VPN in their lifetime and 25% had used a VPN in the last 6 months.⁵ In November 2025, Childnet found that 21% of children aged 8 to 17

⁵ [Ofcom data on children aged 11 to 17 and their use of VPNs](#)



said they had used a VPN.⁶ This latter figure is lower than this research's reported figure of 26%, but one based on a wider age range that includes younger children less likely to have encountered VPN technology.

Figure 1: VPN awareness and use by age group



Source: B03a/B03b/B03c. "Which of the following have you ever heard of / ever used / used in the last 3 months?"
Base: all respondents (n=2,299)

Around a quarter of parents indicate VPN usage in their household

Parents were asked whether there was VPN usage in their household, and whether this was at a Wi-Fi or device level. 25% of parents indicated use of VPN in their household (either personal or use by others). Of those who said their household used a VPN, 34% indicated it was set up at a Wi-Fi level to apply to all devices, 30% indicated it was set up at a Wi-Fi level but used by only some devices, and 41% indicated it was set up on specific devices.

Parental knowledge of VPN usage varies

Among children who said they had used a VPN in the last three months, 78% had parents who were aware of VPN usage in their household, with 22% who were not aware.

Among children who have not used a VPN before, 8% had parents who said there was VPN use in their household, although this was more likely to be on specific devices.

In 17% of households, both the child and parent indicated any VPN use. In 9% of households, the child said they had used a VPN and their parent has not indicated use in the household. In 5% of

⁶ [Childnet research on children and young people's use of VPNs](#)



households, the parent indicated VPN use but the child did not report using one themselves. In 68% of households, no VPN usage has been indicated at all by parent or child.

VPN use without parental knowledge rises with age

The pattern of independent use (where a child reports using a VPN, but their parent does not report a VPN in the household) is particularly pronounced among older teenagers. 15% of 16- to 17-year-olds fall into this category compared to 9% of all respondents.

Frequent use is the norm among children who have used a VPN in their lifetime

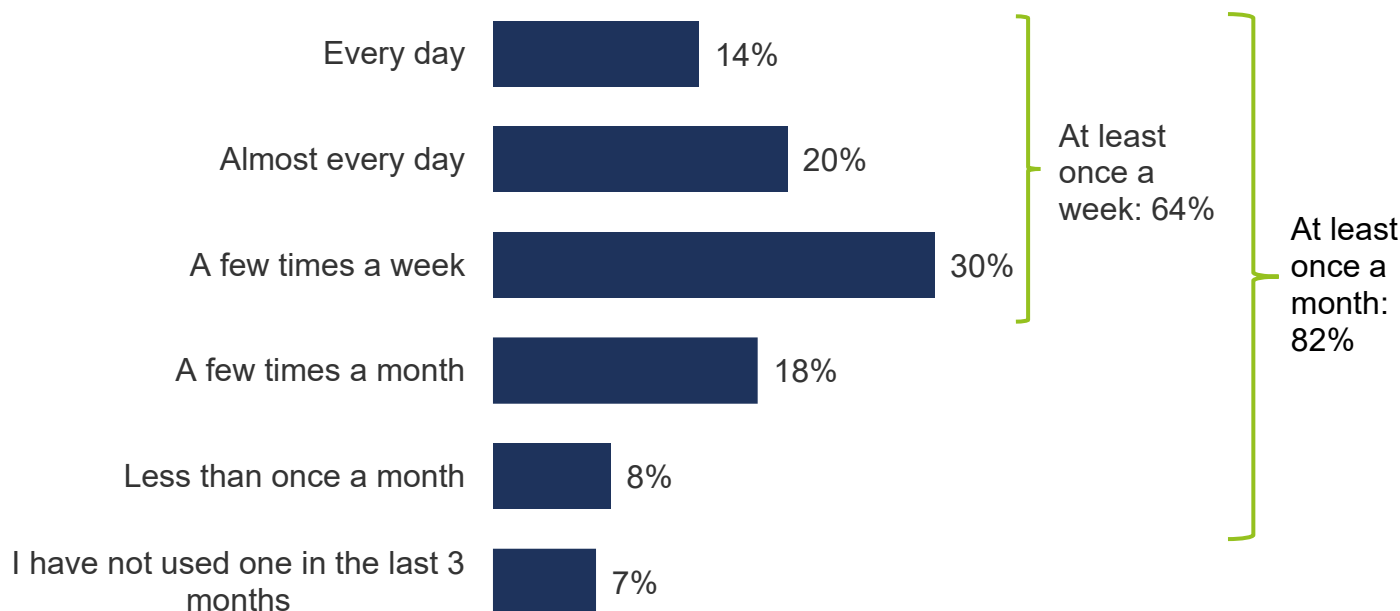
Taken together, just under two-thirds of those who have used a VPN in their lifetime (64%) use one at least once a week.⁷ Breaking this down, 14% of users say they use one every day, a further 20% almost every day, and three in ten (30%) a few times a week.

There is a smaller proportion of less frequent users, with just under a fifth (18%) of lifetime users using a VPN a few times a month. This brings the proportion of users who use a VPN at least monthly to over eight in ten (82%).

Only 8% of lifetime VPN users say they use one less than once a month, and 7% said it has been over 3 months since they last used a VPN.

The frequency of VPN use differs by age group. The proportion using a VPN every day is highest among 16- to 17-year-olds (18%), whereas daily use among 13- to 15-year-olds is notably lower (11%).

Figure 2: Frequency of use among VPN users



⁷ Those who said they have ever used a VPN were asked this question, as well as children who did not disclose VPN use early in the survey but claimed to have 'used tools or setting' akin to VPN tools later on.



Source: E01. “How often do you use a VPN when online?” Base: all children who use VPNs currently or have ever used (n=849).

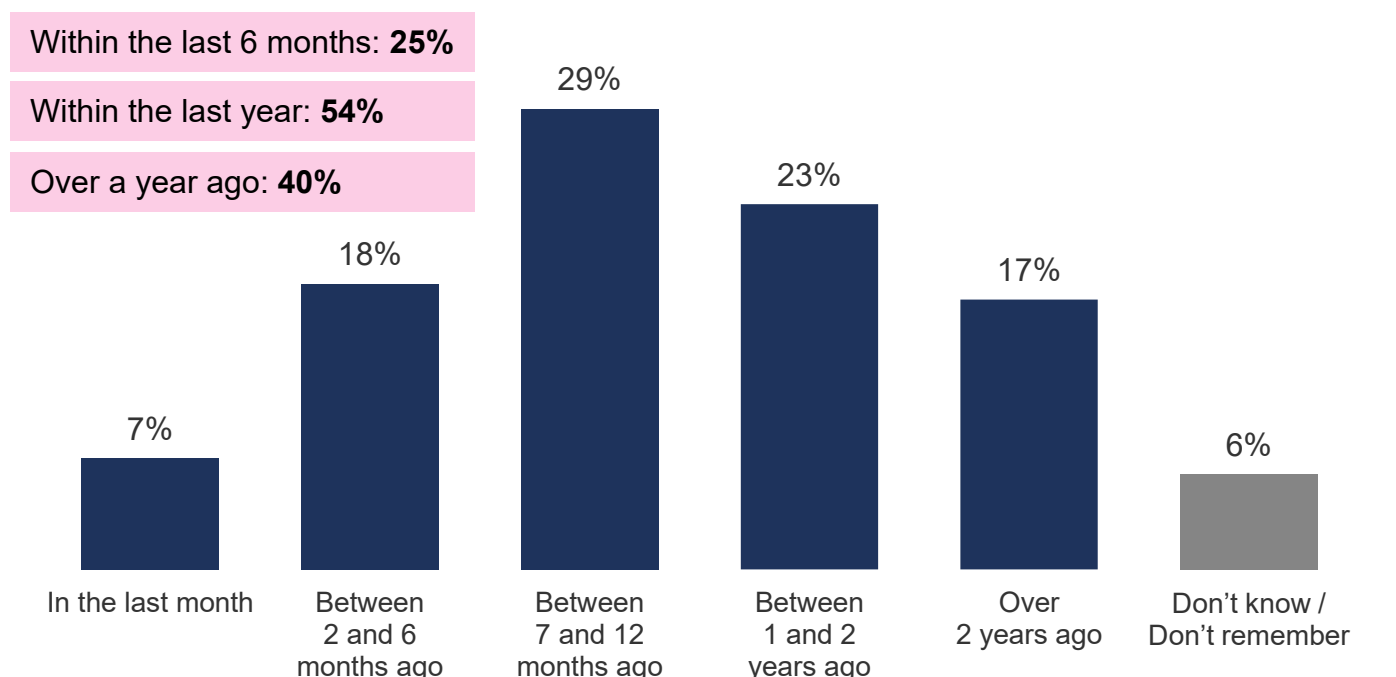
Most VPN users say they started within the last year

Over half of children who currently or have used a VPN in their lifetime (54%) say they started within the last twelve months, and around three-quarters (77%) say they started within the last two years.

Breaking this down further, 7% of VPN users reported starting to use a VPN in the last month, 18% between two and six months ago, and 29% between seven and twelve months ago. 23% said they started using VPNs one to two years ago and 17% more than two years ago. 6% could not recall when they first started using a VPN.

Older children are more likely to have used VPNs for a longer amount of time, indicating that many adopted VPNs in their early-to-mid teens. Just under half of 16- to 17-year-olds (47%) reported starting to use a VPN over a year ago, compared with around a third of 11- to 12-year-olds (35%).

Figure 3: When did children start using VPNs?



Source: E02. “When did you start using a VPN?” Base: all children who currently or have ever used a VPN (n=849).

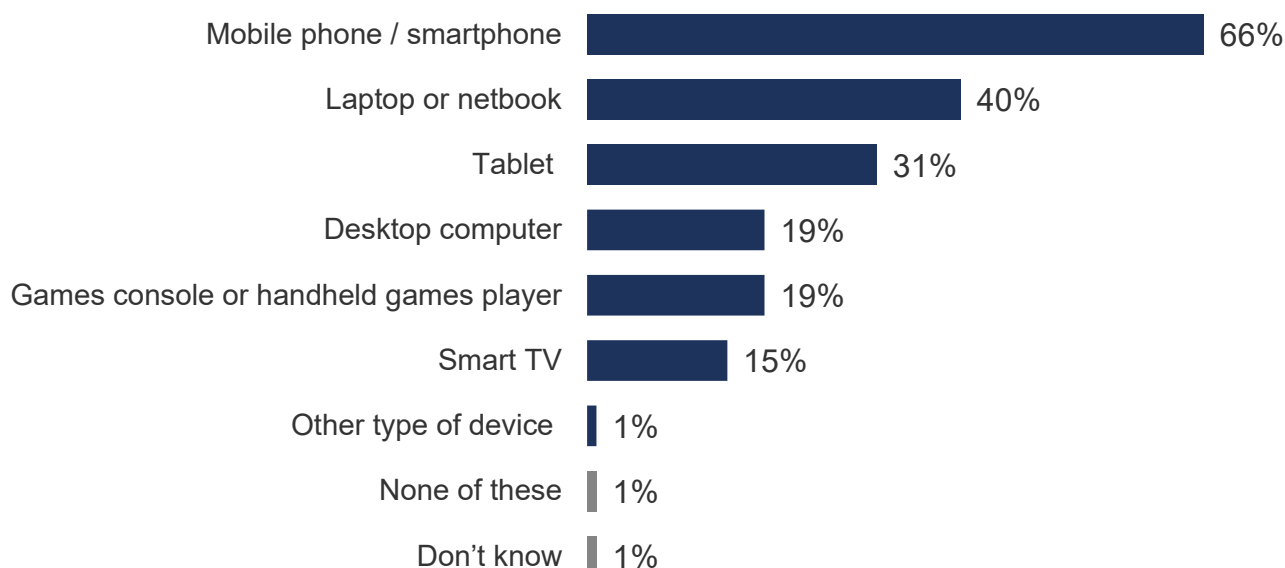
Smartphones are the main device for VPN use

Smartphones are the most common devices children use a VPN on. Two-thirds of children who have used a VPN (66%) say they use it on a mobile phone or smartphone, followed by laptops for four in ten (40%) and tablets at just under a third (31%). Desktop computers and games consoles are each used by around a fifth (19%), while 15% indicated they've used a VPN on a Smart TV. This hierarchy closely mirrors the wider picture of children's device use.



Tablet use for VPNs is notably higher among younger children. 43% of 11- to 12-year-olds who have used a VPN do so on a tablet, compared with 26% of 16- to 17-year-olds. This reflects the broader pattern of tablet use declining as children move into their mid-teens and increasingly rely on phones and laptops.

Figure 4: Devices children use VPNs on



Source: E03. "Which of the following device(s) do you use a VPN on?" Base: all children who use or have ever used a VPN (n=849)

Privacy is the main reason children give for using a VPN

Children report using VPNs for a range of reasons. While no single motivation dominates, answers cluster around reasons related to internet privacy and accessing content.

The most common reason children give for using a VPN is to keep their online activity private, selected by three in ten (30%) of those who have used a VPN in their lifetime. 23% also say they use VPNs to feel safer online by keeping their personal information hidden.

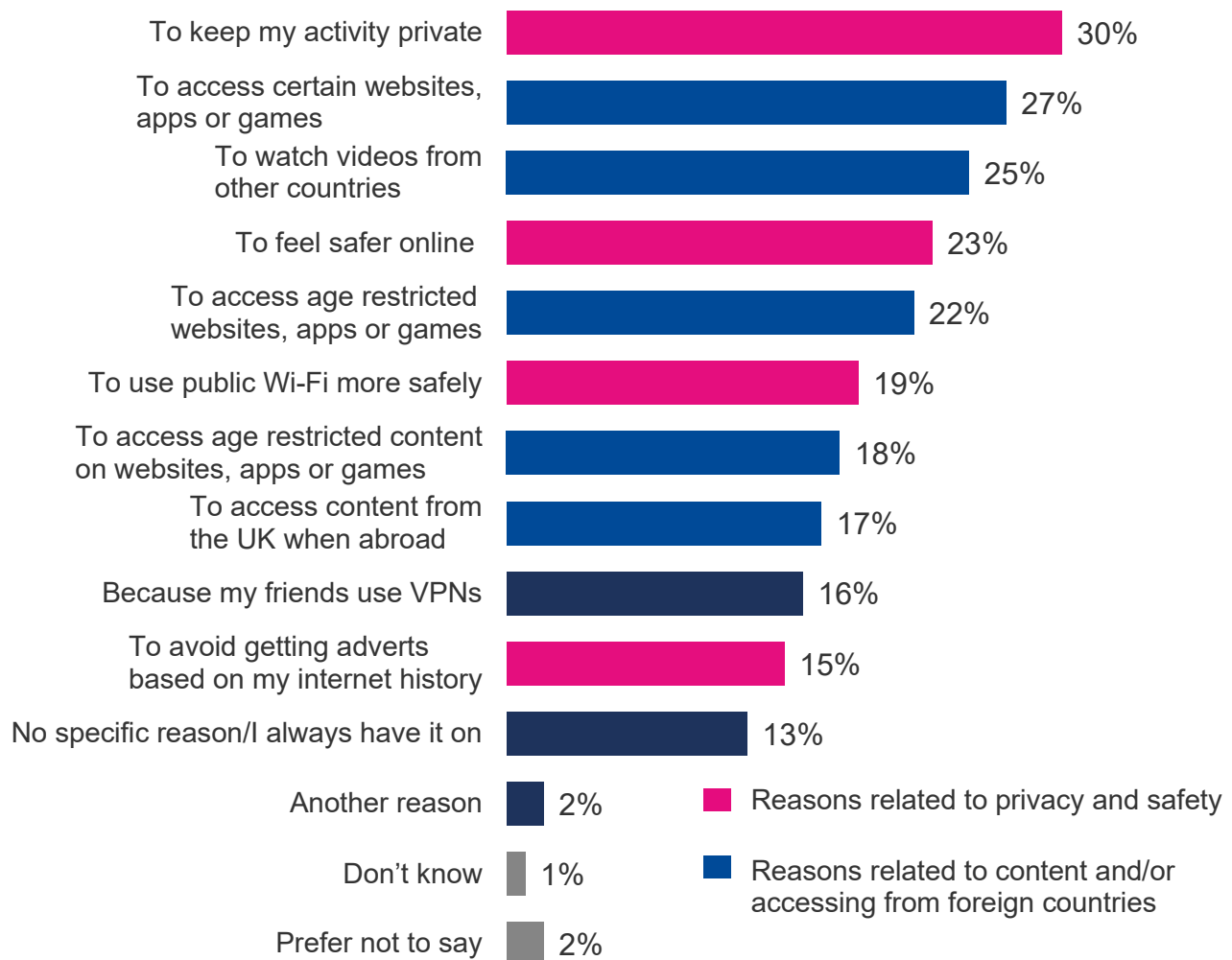
While privacy is the main motivation cited, around a quarter of VPN users also indicated they used it to access certain websites, apps or games (27%) or watch content from other countries (25%). Around a fifth (22%) say they use a VPN to access age-restricted websites, apps or games and a similar proportion (19%) mention using a VPN to access public Wi-Fi more safely or accessing age-restricted content on platforms they already use (18%).

This latter reason refers to instances where the platform itself is not age-restricted but may include blocks on age-restricted content. A notable minority indicate accessing UK content when abroad as a reason for using VPNs (17%), as well as the influence of friends who also use VPNs (16%), and avoiding adverts based on their browsing history (15%). Finally, 13% say they have no specific reasons for using a VPN or always leave it on.

The range of motivations suggests that children use VPNs for a variety of purposes. Children selected an average of over two answers for this question.



Figure 5: Reasons for VPN use



Source: E04 / E05. "People may use VPNs for different reasons. Which of the following, if any, are reasons you use a VPN?" Base: all children who use or have ever used a VPN (n=849)

Reasons vary by demographics and VPN situation

Children from higher socioeconomic backgrounds (ABC1) are significantly more likely than those from C2DE households to cite several motivations: accessing certain websites, apps or games (31% compared with 20%), feeling safer online (27% compared with 17%), and accessing UK content when abroad (20% compared with 11%).

How a VPN is set up also shapes the reasons children give for using one. Where a parent has indicated a VPN is set up on all home devices, children are significantly more likely to say they have no specific reason for using it and simply leave it on (20%, compared with 10% of children in households with no VPN) suggesting that for this group VPN use is a household default.



VPN use to access specific content most often reflects content being unavailable in the UK

Among the 27% of VPN users who say they use one specifically to access certain websites, apps or games, the most common explanation is that the content was not available in their country, cited by over half of those asked (53%). Two in five (41%) say they were not old enough to access the content in question, and a similar proportion (40%) say it was blocked on their school or home network. A small number (5%) cite another unspecified reason.

VPN users are more likely to rate online privacy as very important

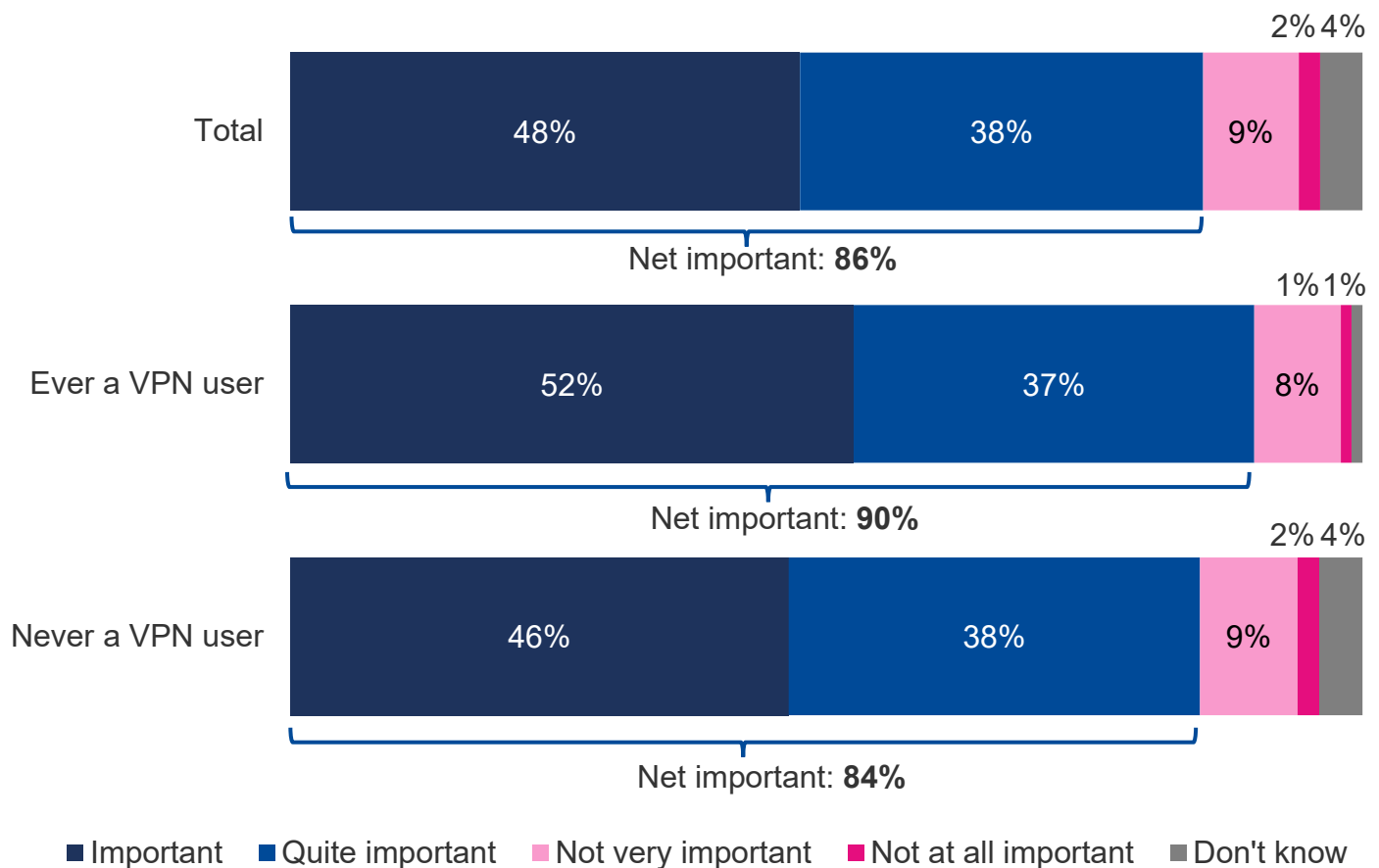
Across all children we surveyed, the vast majority (86%) say it is important to them that their online activity is private. 48% of children say it is very important and 38% say it is quite important. Only one in ten (11%) children say their online activity being private is not important to them. The value placed on privacy increases with age; 89% of 16- to 17-year-olds say it is important compared to 81% of 11- to 12-year-olds.

Among children who have ever used a VPN, the importance placed on privacy is even higher. 90% say it is important that their online activity is private, with over half (52%) saying it is very important. This compares with 84% among children who have never used a VPN, and with only 46% saying it is very important.

It is important to note the possible age-effect of this relationship, as older children (who place more importance on privacy) are also more frequent users of VPNs.



Figure 6: Perceived importance of online privacy



Source: B06. "How important is it that your activity is private?" Base: all respondents (n=2,299), all who have ever used a VPN (n=762), those who were never a VPN user (n=1,450)

Children have a widespread definition of "online privacy"

When asked what "online privacy" means to them, children most often point to two concerns: keeping their personal information hidden (40%) and keeping their accounts safe from being hacked (40%).

Around a third (34%) indicated stopping strangers contacting them and a similar proportion cite keeping photos or videos from being shared without permission (31%) and not sharing their location with others online (29%).

Around a quarter mention keeping their online activity private (27%) and choosing who sees what they share or upload (25%), while just under a quarter (23%) highlight not sharing their real name or age. Fewer children point to being able to control or delete their information online (17%) or companies not collecting or using their personal data (12%).

On average, children selected almost three answers, indicating that children's definition of 'online privacy' is multidimensional.



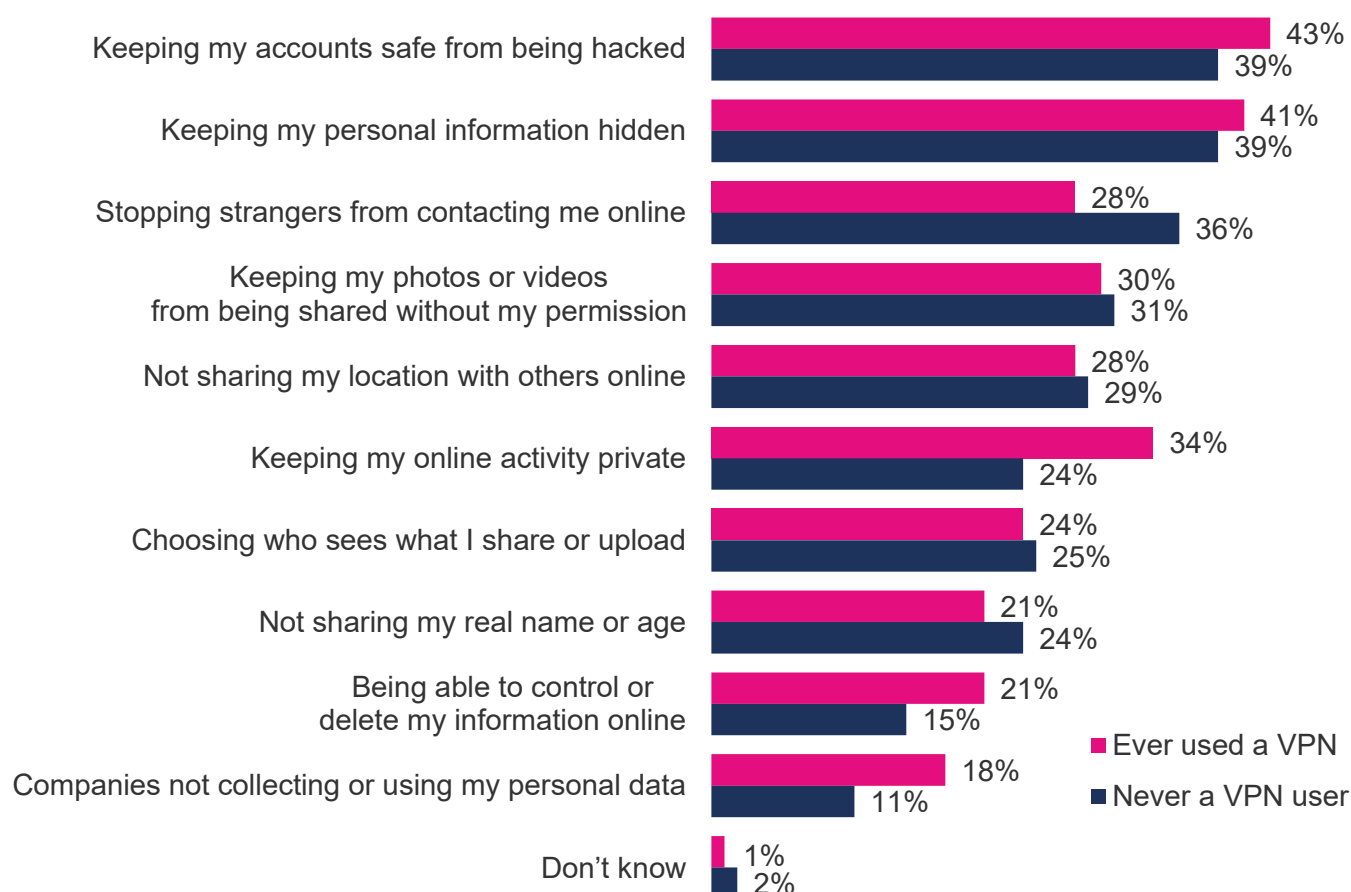
What “online privacy” means varies by age and by VPN use

Definitions of privacy shift with age, reflecting children's developing relationship with the internet. Younger children are more likely to see “online privacy” as stopping strangers from contacting them (42% of 11- to 12-year-olds mention this, compared with 27% of 16- to 17-year-olds) and not sharing their real name (30% of 11- to 12-year-olds, compared with 19% of 16- to 17-year-olds). In contrast, older children place greater emphasis on keeping their personal information hidden (43% of 16- to 17-year-olds, compared with 35% of 11- to 12-year-olds).

Children who have used a VPN define privacy similarly to children who have never used one, except for some areas. VPN users are more likely than average to associate privacy with keeping their online activity private (34%, compared with 24% of non-users), being able to control or delete their information online (21%, compared with 15%), and companies not collecting or using their personal data (18%, compared with 11%).

These findings align with the core functions commonly associated with VPNs, so it's unsurprising that VPN users are more likely to define privacy in terms of control over what is visible and traceable online.

Figure 7: How children define online “Privacy”



Source: B07. “Which aspects of online privacy matter most to you?” Base: all who have ever used a VPN (n=762); all who have never used a VPN (n=1,537)



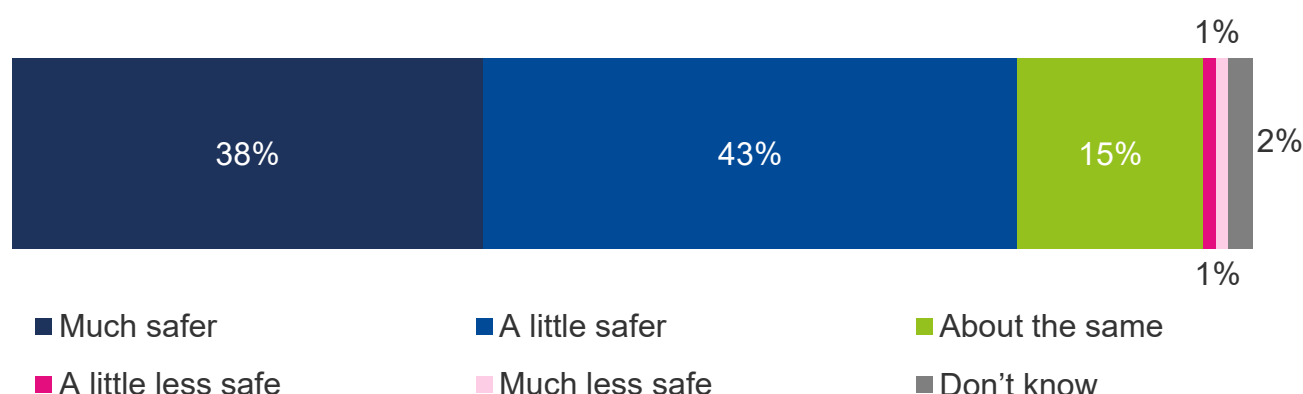
Most children who use a VPN feel safer for doing so

Over eight in ten children who use a VPN (81%) say it makes them feel safer online. Within this, 38% say it makes them feel much safer, and 43% report feeling a little safer. 15% say using a VPN makes no difference to how safe they feel online, and very few report feeling less safe / much less safe (2%).

Younger VPN users are more likely than older VPN users to report that VPNs make them feel safer online. Nearly nine in ten (89%) of 11- to 12-year-olds who use a VPN say it makes them feel safer, compared with 78% of 13- to 15-year-olds and 82% of 16- to 17-year-olds.

Under the UNCRC, children have a right to privacy.⁸ The findings suggest that privacy is an important consideration for many children who use VPNs.

Figure 8: The extent to which VPNs make children feel safer online



Source: E08. "Does using a VPN make you feel more safe or less safe online?" Base: all children who use or have used VPNs (n=849)

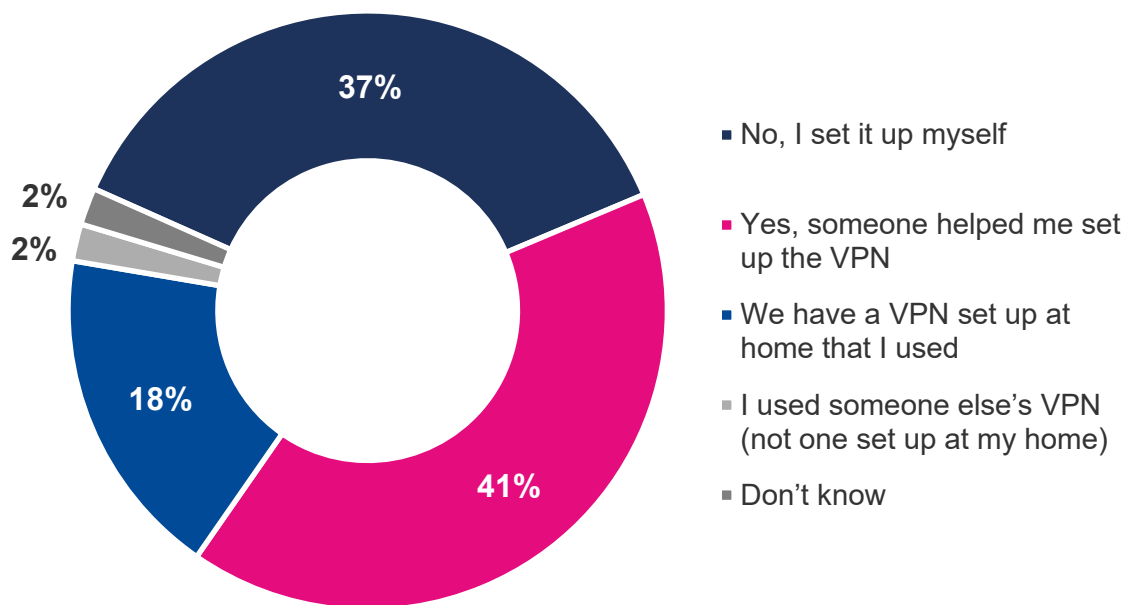
Children take different routes to setting up a VPN

We asked children who used VPNs whether anyone had helped them set up the VPN they use. Nearly two in five set up the VPN themselves (37%), while 41% had help from someone else. 18% used a VPN already set up at home, and a minor proportion (2%) used someone else's VPN rather than setting one up.

⁸ [UNICEF document summarising the UN Convention on the Rights of the Child \(UNCRC\)](#)



Figure 9: Help received to set up the VPN



Source: E06a. "Did anyone help you set up the VPN?" Base: all children who use VPNs currently or have ever used a VPN (n=849)

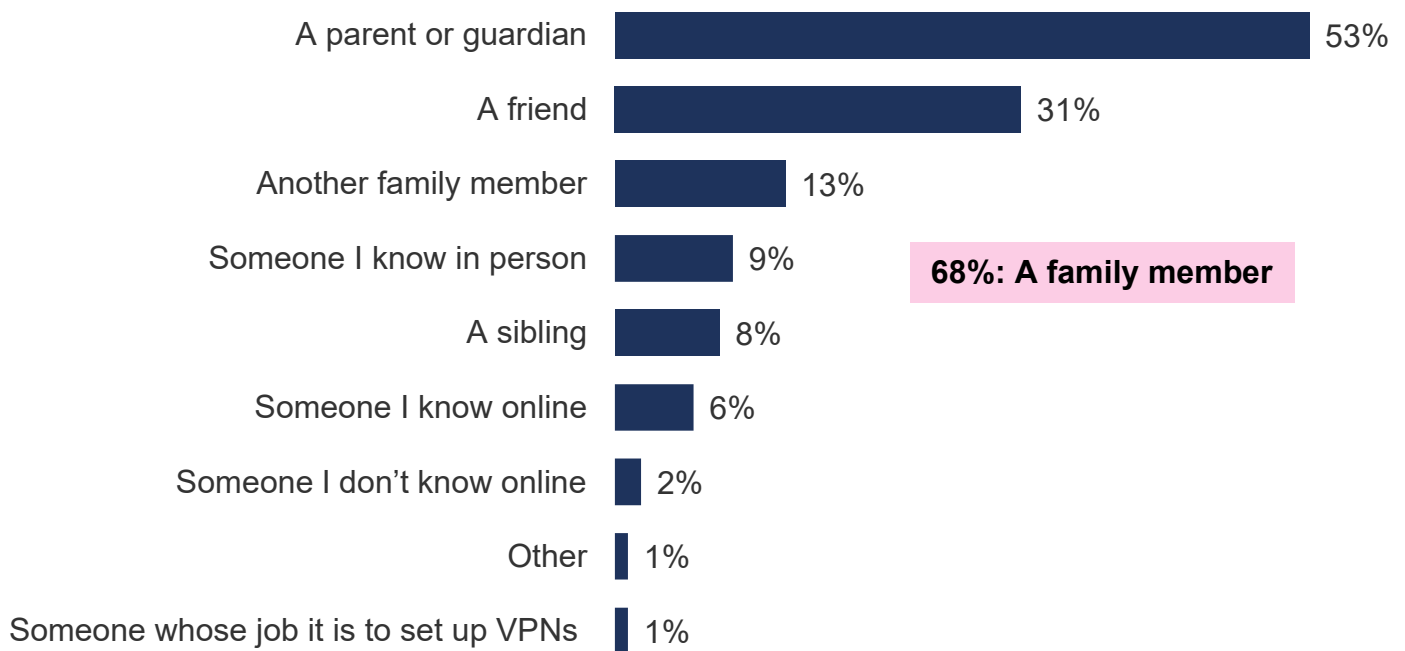
Parents are the main helpers for setting up a VPN

Of those who had help, more than half (53%) were helped by a parent or guardian. This equates to a fifth (22%) of VPN users having help from a parent or guardian to set up the tool.

Friends were the source of support for those who had help for just under a third (31%), followed by other family members (13%) and siblings (8%).

Taken together, family members account for around two-thirds (68%) of helpers. Very few said that it was people outside of family or friends, with 6% saying they had help from someone they knew online, and 2% saying they were helped by someone they did not know online.

Figure 10: Who helps set up VPNs?



Source: E06b. "Who helped you set up the VPN?" Base: all those who had help setting up a VPN (n=341)

Older children and boys are much more likely to have set a VPN up themselves

Younger children more often have a supervised route to VPN access, while older teenagers are more likely to do so independently of their guardians. While a quarter (24%) of 11- to 12-year-olds who use a VPN set it up themselves without help, this increases to 36% of 13- to 15-year-olds but peaks at just under half (46%) of VPN using 16- to 17-year-olds. Meanwhile, younger children are more likely to have had someone help them; around half (49%) of 11- to 12-year-olds received assistance compared to a third (34%) of 16- to 17-year-olds.

This likely reflects greater independence granted to 16- to 17-year-olds as parents of 16 to 17s are a lot more likely to say they do not try to limit what their children do on their devices/online (22% vs. 6% for 13 to 15s and 2% for 11 to 12s).

There is also a significant gender difference. Boys are considerably more likely than girls to have set up a VPN themselves (44% of boys compared with 28% of girls). This gap may relate to broader patterns of digital confidence, as boys are more likely to have heard of VPNs, adblockers and anti-virus software than girls.

Children who set up their devices on their own are less likely to be from households that are 'doing well' financially

Beyond age and gender, children who set up a VPN themselves are a distinctive group in several respects. They are more likely to come from a household where no adult reports household usage of a VPN (47%).



There is also a link to financial circumstances: children in households classified as doing well financially are less likely to have set up a VPN themselves (31% compared to 37% of all VPN users) and are more likely to say they have a VPN already set up at home that they use (22% compared to 18% of VPN users) which may reflect differences in digital independence across household types.

VPN setup interacts with parental awareness of VPN usage

The type of VPN setup a parent reports in the household is closely linked to how the child reports setting up a VPN and who helped them. Where a parent says they have configured a VPN across all home devices, over a third of children (35%) simply used the VPN already in place at home.

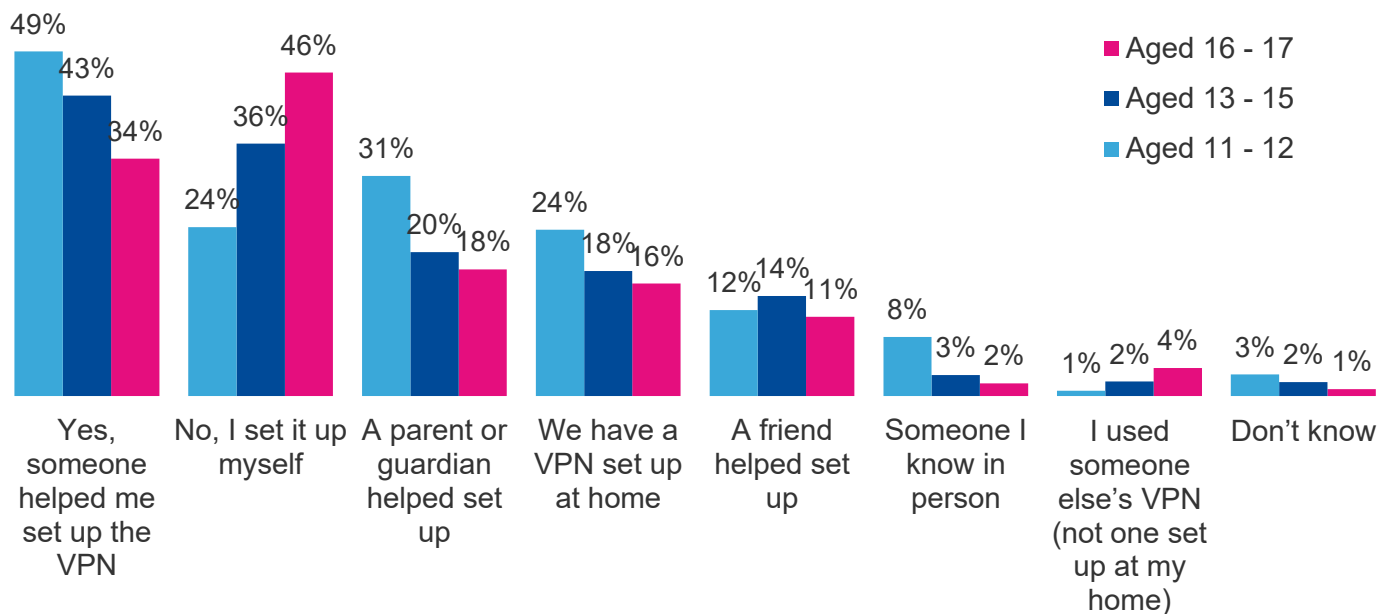
When these children did have help, it was indicated to be overwhelmingly from family: 68% said they were helped by a parent or guardian, and 86% by a family member of some kind. For this group, VPN use most closely resembles a household-wide feature provided and configured by a parent.

Device-level setups appear to involve a greater degree of parental and child involvement. Where parents say a VPN is set up only on specific devices, the picture is broadly similar: two-thirds (66%) of children who had help say they were assisted by a parent. However, children in this group are more likely to have set up a VPN themselves (37%) than those in households where parents say a VPN is set up on all devices (20%).

A different picture emerges for children in households where no parent reports using a VPN. Nearly half of children in these types of household (47%) say they have set up their VPN themselves. Among those children who did receive help, friends become the dominant source of support (48%), and these children are more likely to have been helped by someone they know online (11%), or someone they do not know online (5%).



Figure 11: Help with setting up VPNs by age group*



Source: E06a. "Did anyone help you set up the VPN?" Base: all children who use or have ever used a VPN (849) / E06b. "Who helped you set up the VPN?" Base: all children aged 11 to 12 who had help setting up a VPN (n=134), 13 to 15 (n=411), aged 16 to 17 (n=304)

*Children were allowed to indicate multiple sources of help for E06b

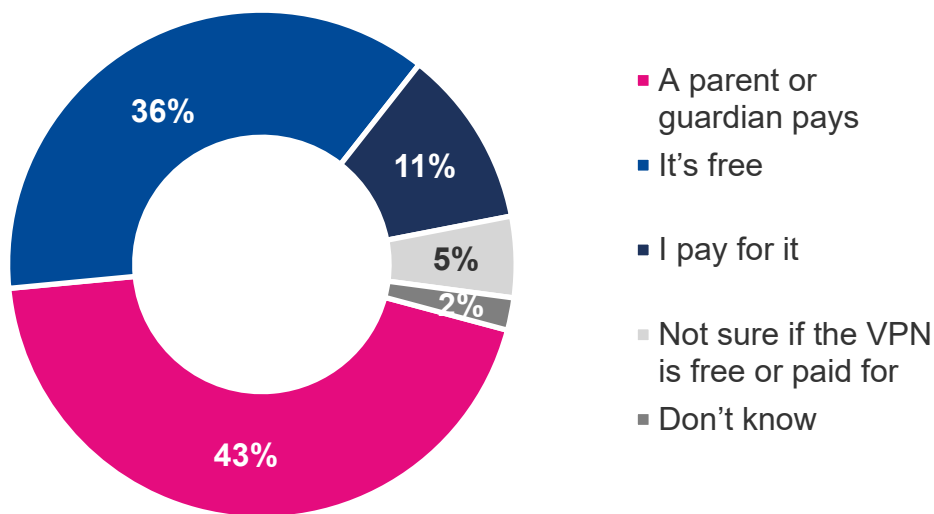
Parents most often pay for their child's VPNs

Among children who currently use a VPN, the most common arrangement is for a parent or guardian to pay, which is the case for two in five (43%). Over a third (36%) say the VPN they use is free. Only one in ten (11%) current VPN users say they pay for it themselves. 5% are unsure whether their VPN is free or paid for.

Boys are significantly more likely to say their VPN is free (40%) compared with girls (31%), while girls are more likely to say a parent pays (48% of girls compared with 39% of boys).



Figure 12: Who pays for the VPN?



Source: E07. "Who pays for the VPN you use?" Base: all children who currently use a VPN (n=777)

Free VPN usage is mainly among 15- to 16-year-olds

The proportion saying their VPN is free shifts across the groups. Among the youngest users (11- to 12-year-olds), half (50%) say a parent pays for their VPN and around a quarter (26%) say it is free. Free VPN use rises through the early to mid-teens, peaking among 15- and 16-year-olds (45% on average), while the proportion saying a parent pays dips to its lowest point among 14- and 15-year-olds (36% on average).

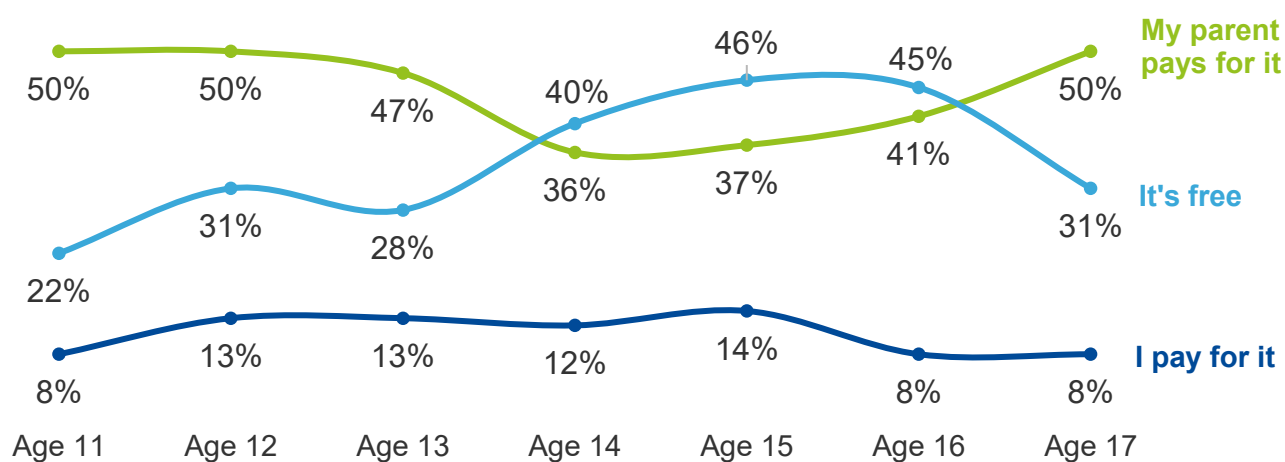
Older teens and boys in general are more likely to pursue VPNs independently in both set up and financing, which could explain the higher use of free VPNs. Further to this, 64% of children who set up a VPN by themselves report that the tool they use is free, suggesting a subset of children who are acquiring and using VPNs mostly outside of parental oversight or financial involvement.

Where parents do not indicate a VPN in the household, free options are most common

For children in households where no parent reports using a VPN, nearly half (48%) say the VPN they use is free. These children are also significantly more likely to say they pay for a VPN themselves (15%).



Figure 13: Method of paying for VPN by age



Source: "Who pays for the VPN you use?" Base: all children who currently use a VPN (n=777)



Section 2: Encountering age checks

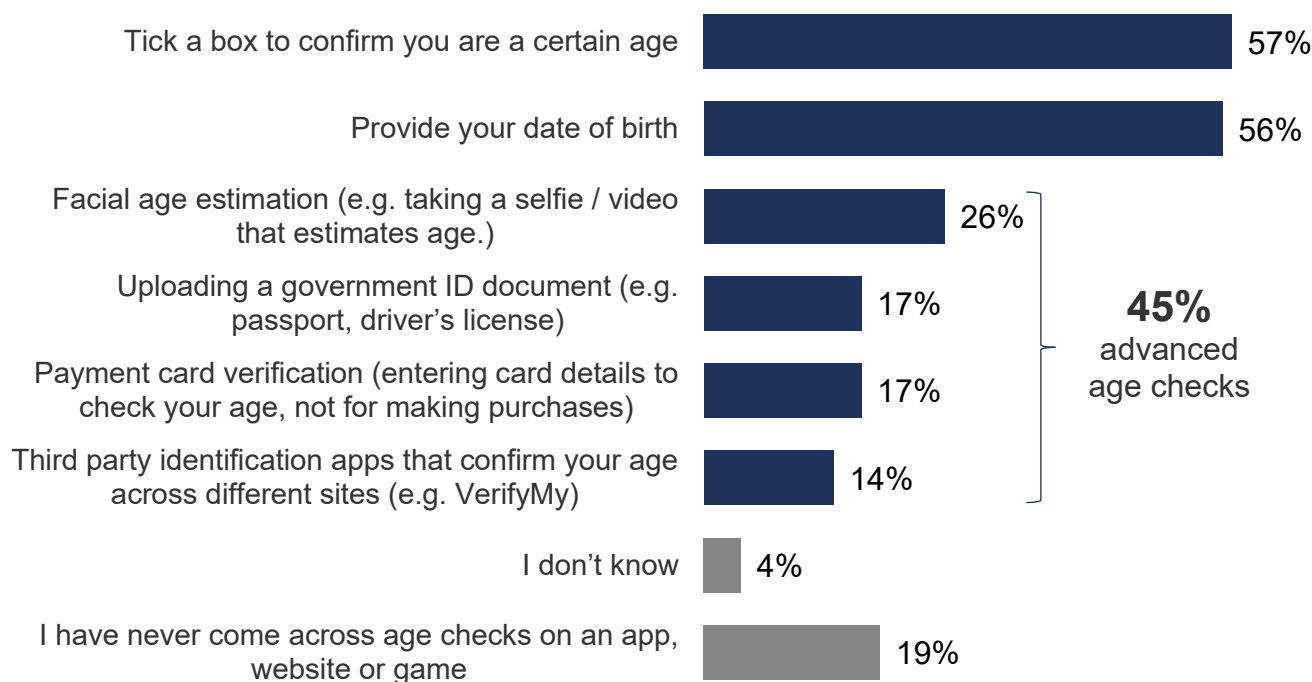
Children have a varied experience of age checks online

The age checks children most commonly report being asked to complete are ticking a box to confirm their age (57%) and entering a date of birth (56%).⁹ These are the age check methods children encounter most frequently. This may reflect the fact that many online services, including social media platforms, rely on self-declaration methods to determine whether users meet minimum age requirements which are often set at age 13.

In contrast, advanced age checks are encountered less commonly by children. 45% of children have experienced any of the more advanced age checks. Facial age estimation has been encountered by just over a quarter of children (26%), while uploading a government ID document (17%), payment card verification (17%) and third-party identification apps (14%) are each encountered by fewer than one in five children.

Notably, around one in five of all children (19%) say they have never come across an age check at all.

Figure 14: Age checks encountered



Source: C02. "Which, if any, of the following types of age checks have you been asked to do when using a website or game?" Base: all respondents (n=2,299)

⁹ These types of checks are often used on websites that require the user to be 13 or older. Many social media services have these types of age checks in place.



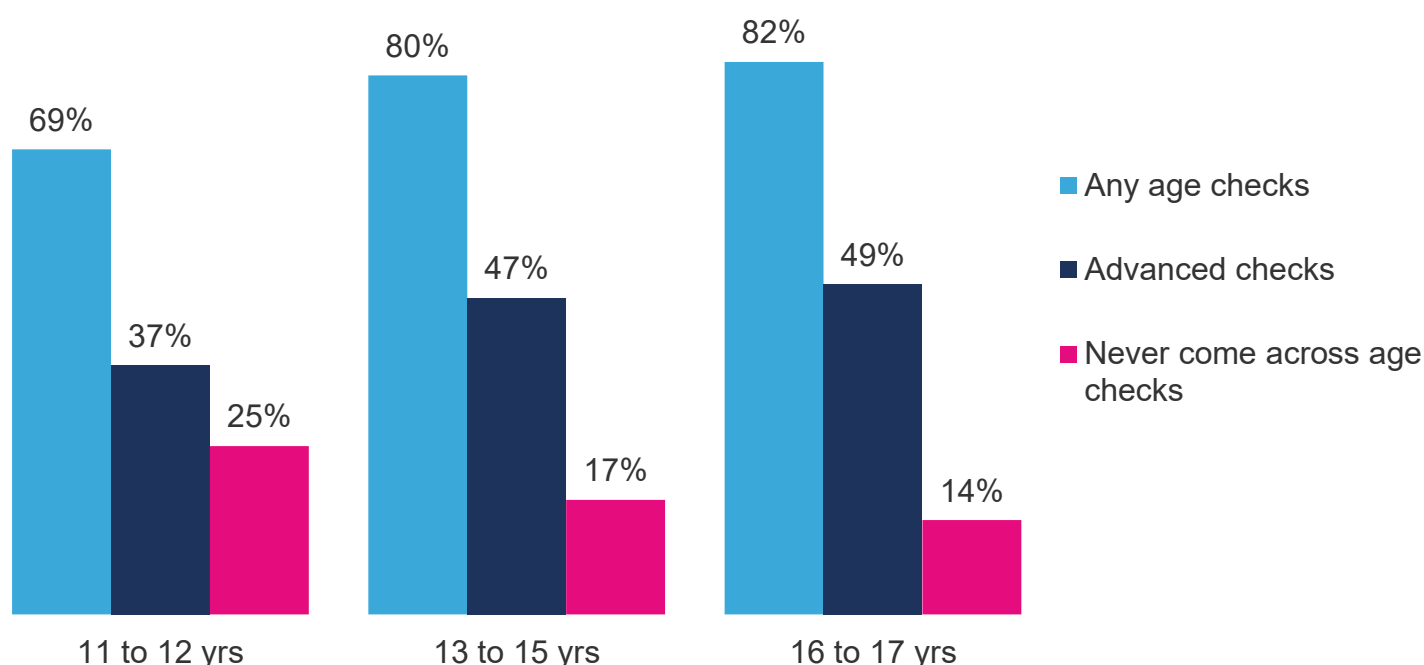
Older children encounter a wider range of checks

Age shapes children's experience of age checks in different ways. Younger children are the most likely to say they have never encountered an age check at all (25% of 11- to 12-year-olds, compared with 14% of 16- to 17-year-olds).

Older children are more likely to have encountered age checks, experience a wider range of check types, and come across more advanced age assurance methods.

Uploading a government ID is most commonly encountered by 16- to 17-year-olds (25%, compared with 16% of 13- to 15-year-olds and 12% of 11- to 12-year-olds), while payment card verification has been encountered by 22% of 16- to 17-year-olds (compared with 18% of 13- to 15-year-olds and 13% of 11- to 12-year-olds).

Figure 15: Encountering of advanced checks* by age



Source: C02. "Which, if any, of the following types of age checks have you been asked to do when accessing an app, website or game?" Base: all respondents (n=2,299)

*Advanced age checks include uploading a government ID document, facial age estimation, third-party identification apps and payment card verification

VPN users have more extensive experience with advanced age checks

Children who currently use a VPN are more likely to have experienced advanced age checks (66%) compared with those who have never used a VPN (38%). The result for VPN users cannot only be explained by the older age profile of VPN users, with only 49% of 16- to 17-year-olds experiencing advanced age checks. The advanced check VPN users are most likely to have encountered are facial age estimation (42%) and uploading a government ID document (31%).



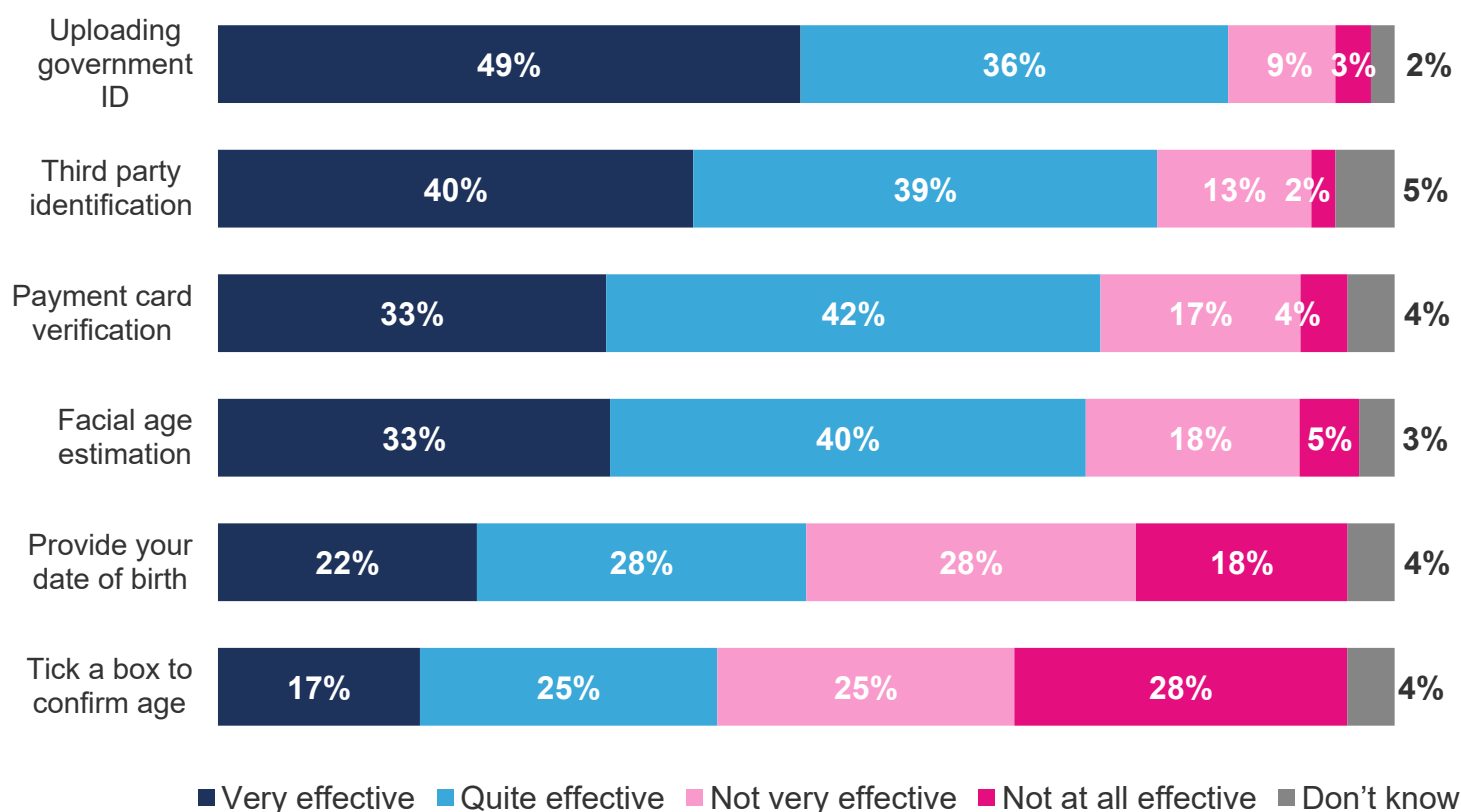
Advanced checks are seen as far more effective than ticking a box or entering a date of birth

Children have varying opinions about which age checks are most likely to be effective in stopping people their age from accessing content intended for older users. Uploading a government ID is rated effective by 86% of children who have encountered it, the highest rating of any method. This is followed by third-party identification apps (79%), payment card verification (74%) and facial age estimation (73%).

Unsurprisingly, effectiveness drops considerably for the more straightforward age checks methods. Half of those who have provided their date of birth (50%) think it is effective at blocking people their age from accessing content meant for older users, while 46% think it is not effective, and a majority of those who have ticked a box to confirm they are a certain age (54%) think it is not effective. These findings suggest that children are capable of distinguishing between age assurance methods that feel meaningful and those that feel like little more than a formality.

This produces a clear discrepancy. The two checks the higher proportion of children have come across, ticking a box and entering a date of birth, are the two they are least confident actually work. Children are, in effect, being asked to satisfy checks that they themselves regard as easy to ignore or bypass.

Figure 16: Perceived efficacy of age check types



Source: C05. "How effective are the following age checks at blocking people your age from accessing content that is meant for older users?" Base: Floating base among those who have experience of each type of age check



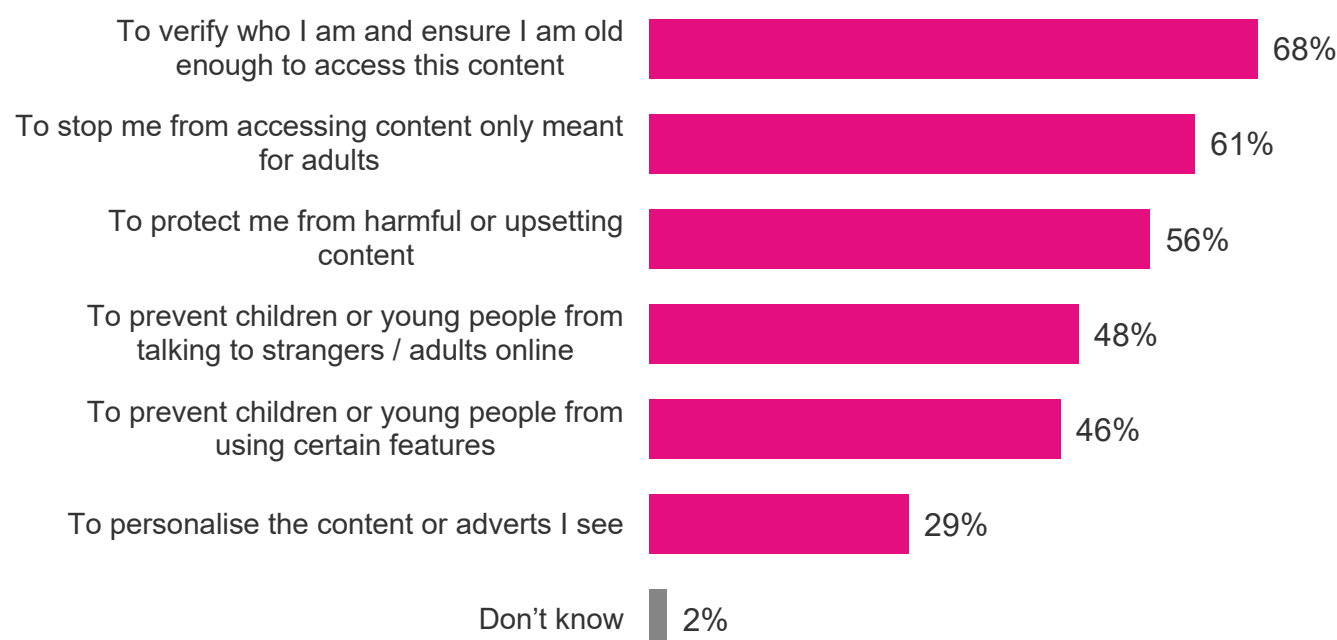
Children are aware age checks are mainly used to confirm they are old enough to access certain content

Among children who have been asked to complete an age check, understanding of their purpose appears relatively high. 68% see them as a way to verify who they are and confirm they are old enough to access certain content, and 61% associate them specifically with blocking content intended only for adults.

A substantial proportion also link age checks to broader safeguarding aims. Around half connect them to protecting children from harmful or upsetting content (56%) and to preventing children from communicating with strangers (48%). This suggests that children do not simply see age checks as arbitrary obstacles, many understand them as part of a wider effort to keep people safe online.

VPN users are more likely to link age checks with personalising the content or adverts they see (34% vs. 27% non-VPN users).

Figure 17: Perceived purpose of age checks



Source: C03. "Why do you think your age was checked online?" Base: All children who have been asked to complete an age check (n=1,875)

Trust in the security of an age check is higher for advanced methods of age assurance

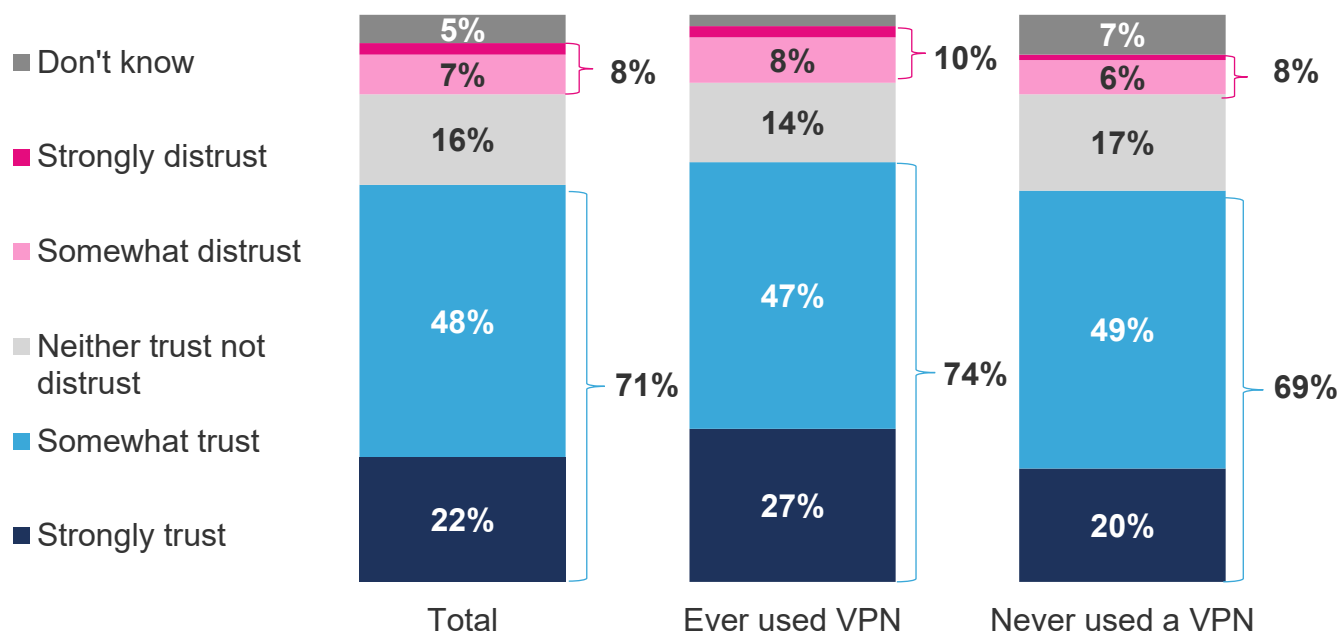
71% of children who have completed an age check say they trust that their information is kept secure. Just 22% express strong trust, while 48% say they somewhat trust it, suggesting cautious acceptance rather than confidence.

Trust is notably higher among children who have encountered the more advanced check types, such as third-party identification apps (80% trust), payment card verification (78%) and government ID (75%).



Children who have used a VPN in their lifetime are slightly more trusting than average when it comes to data security (74%) compared to non-VPN users (69%), which aligns with a broader tendency among this group to feel more comfortable online.

Figure 18: Trust in age checks



Source: C04. "To what extent do you trust or distrust that your information is secure when you've had to give information for age checks?" Base: All children who had been asked to complete an age check (n=1,875); All children who have ever used a VPN (n=697); Children who say they have never used a VPN (n=1098)



Section 3: Bypassing age checks

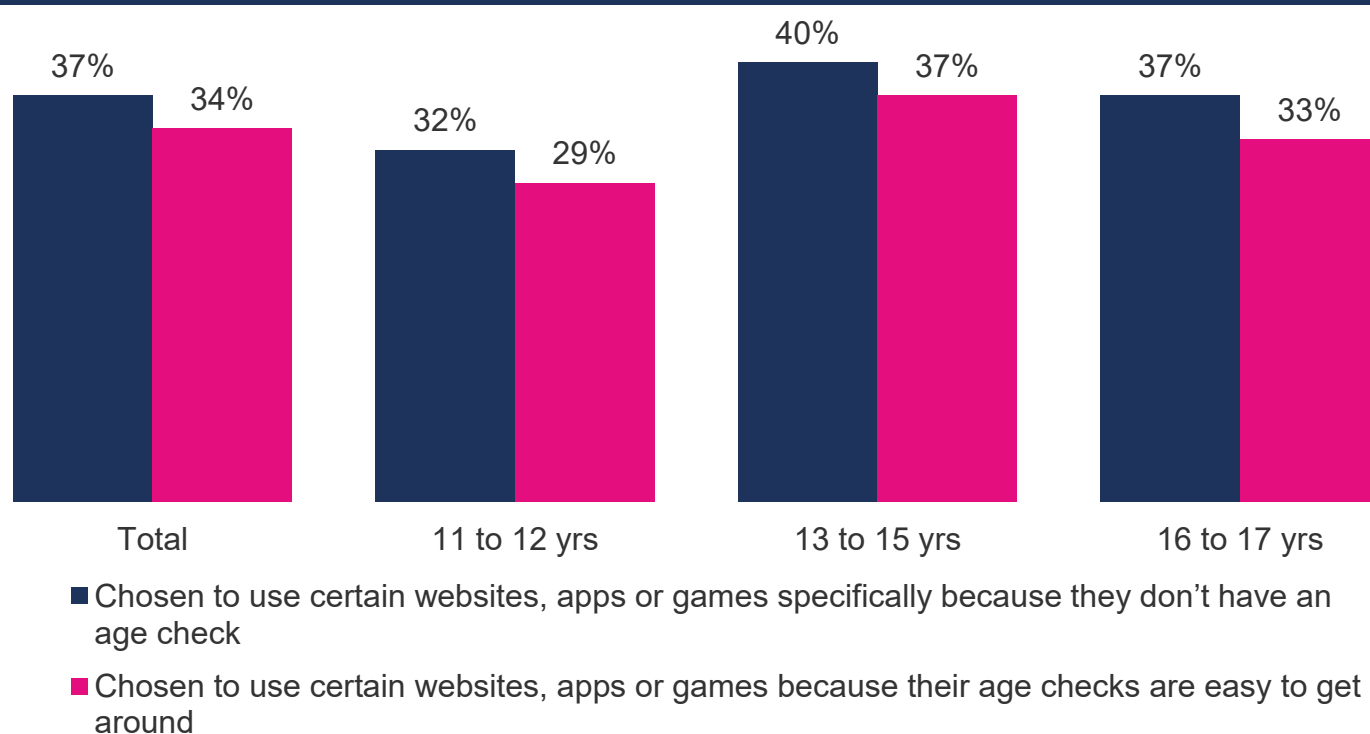
Over half of children have chosen platforms to avoid or get around age checks

Before children even attempt to get past an age check directly, many make choices that avoid them altogether. Over half of 11- to 17-year-olds (53%) say they have deliberately chosen websites, apps or games to sidestep age checks. This includes 37% of children who have picked a platform specifically because it had no age check at all and 34% who have chosen one because they knew the checks would be easy to get around.¹⁰

This behaviour differs by age group. It is most common among 13- to 15-year-olds (58%), although even among the youngest children, almost half report doing it (47% of 11- to 12-year-olds).

Similar differences are seen by gender. Boys aged 13 to 15 are the most likely group to choose certain websites, apps or games to get around an age check (60%), whereas girls aged 11 to 12 are the least likely to report any of these behaviours (46%). VPN users are also more likely to report these behaviours (76%) with non-VPN users less likely (46%), an association that cannot be wholly explained by the older age profile of VPN users.

Figure 19: Age check circumvention by age



Source: D01. "Which of these have you ever done?" Base: all respondents (n=2,299)

¹⁰ The question was phrased to focus on websites, apps or games children have used because of their age-check status, but it is possible children could be inadvertently thinking about a website where the content does not need age gating.

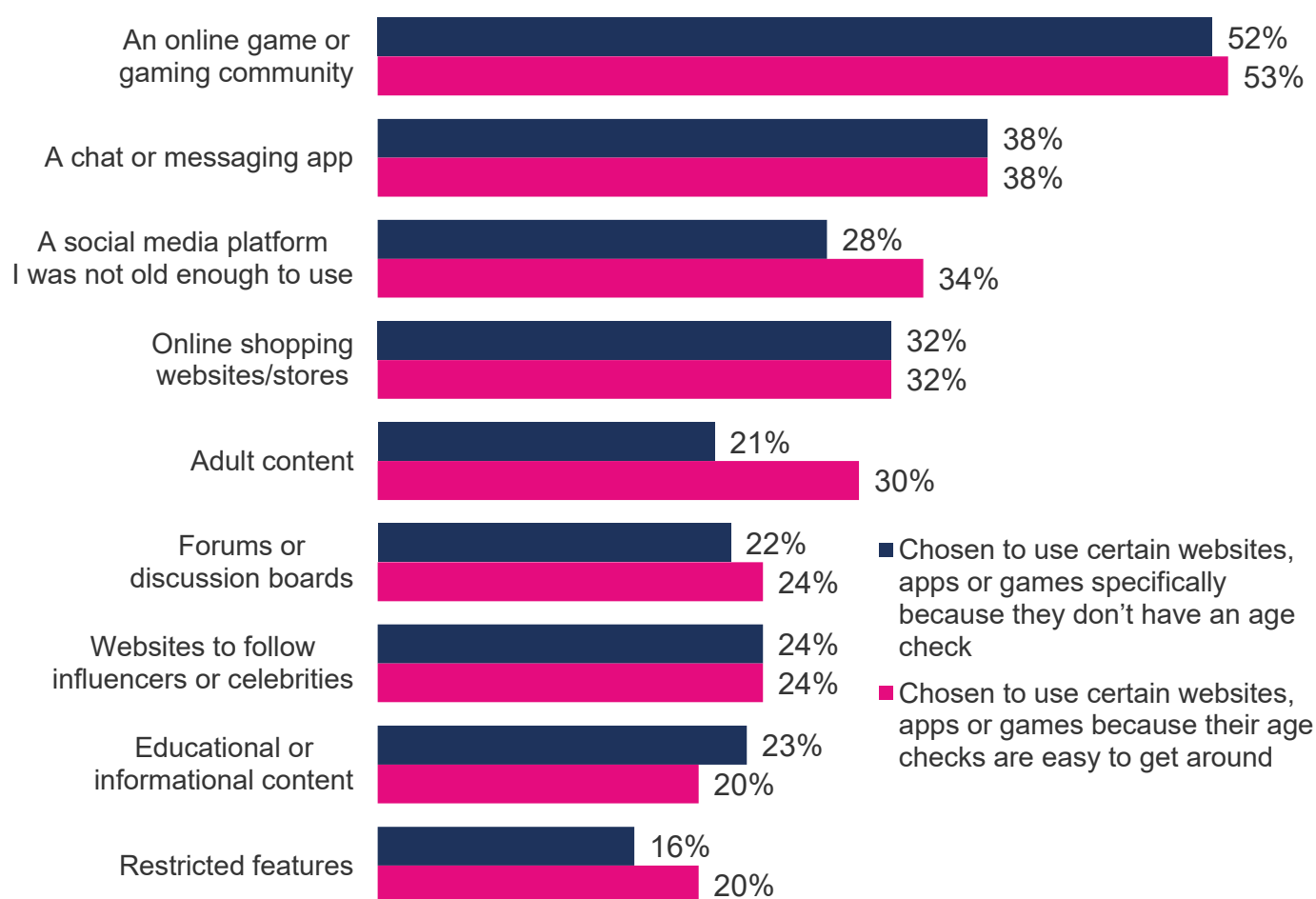
Gaming, messaging and social media are the main services children seek out this way

Among those who picked a platform with no age check, the most common types of content accessed were online games or gaming communities (52%), chat or messaging apps (38%), online shopping (32%) and social media platforms they were too young to use (28%).

Similar patterns are seen among children who chose platforms with weak or easily passed checks, but two categories stand out more strongly in that group: social media they were too young for (34% vs. 28% for platforms with no age checks) and adult content (e.g. 18+ content or violent content) (30% vs. 21% for platforms with no age checks).

These figures cover content and services with very different minimum age requirements. Most of what children sought, such as gaming, chat and messaging apps, forums and social media, typically carries a minimum age of around 13, while restricted features (including live streaming) generally apply from 16 to 18 and adult content is restricted to 18 and over.

Figure 20: Reasons for avoiding age checks or finding easy age checks



Source: D02. "Which type of content have you tried to access by doing the following?" Base: all children who use certain websites, apps, or games because they don't have an age check (n=933), age checks are easy to get around (n=848)



Nearly two in five report successfully getting around an age check

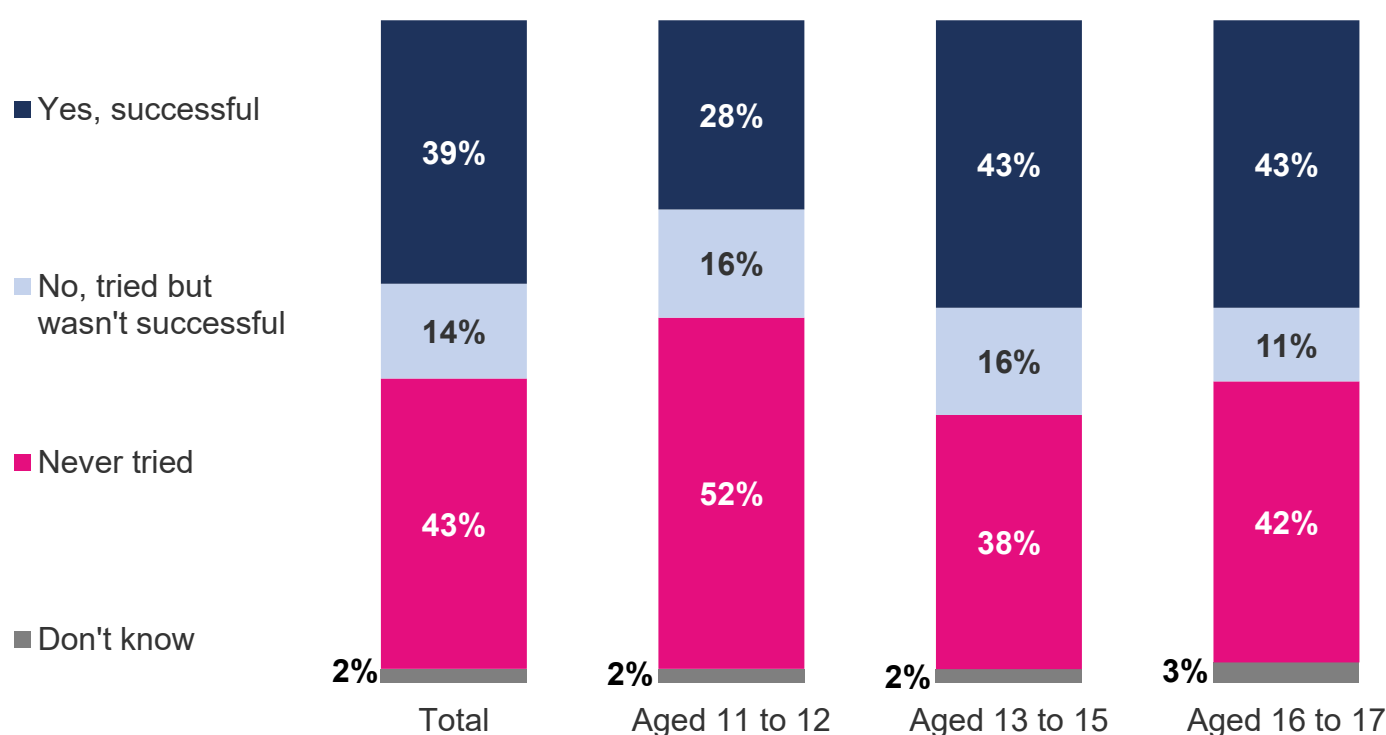
Beyond choosing platforms strategically, many children say they have directly bypassed age checks despite restrictions and succeeded.¹¹ This includes both advanced checks and simpler checks like tick boxes and entering a birth date. 39% of all 11- to 17-year-olds say they have successfully got around at least one age check, and a further 14% have tried but did not manage it. Combining the two, 53% of children say they have attempted to get around age assurance checks at least once.

Success becomes steadily more common with age, rising from 28% of 11- to 12-year-olds to 43% among both 13- to 15- and 16- to 17-year-olds.

Among children who have used a VPN in their lifetime, 56% say they have successfully got around an age check, compared with 33% of those who have never used one. Children who have set up a VPN themselves are more likely to be successful (71%).

Although there is an age effect in success of bypassing age checks, it is not strong enough to explain the full extent of the association between VPN usage and getting around an age check, despite the older age skew of VPN users.

Figure 21: Success of bypassing age checks



Source: D02b. "Have you ever been successful in getting around age checks (i.e. accessing despite age restrictions)?" Base: all respondents (n=2,299), children aged 11 to 12 (n=534), children aged 13 to 15 (n=980), children aged 16 to 17 (n=785)

¹¹ Age checks include "entering your birth date", "asking you to tick a box to confirm you are a certain age", "providing an ID document" or "tools that can guess your age by looking at your face".



Bypassing age checks is associated with a range of age check experiences

Among those who said they had successfully bypassed age checks, 60% had experienced at least one type of advanced age check, including 37% who had encountered facial age estimation, 24% uploading a government ID document, 20% who had experienced third-party identification apps, and 25% who had experienced payment card verification. Those who had bypassed were also likely to have experienced softer age checks such as providing their date of birth (71%) and ticking a box to confirm they are of a certain age (73%).

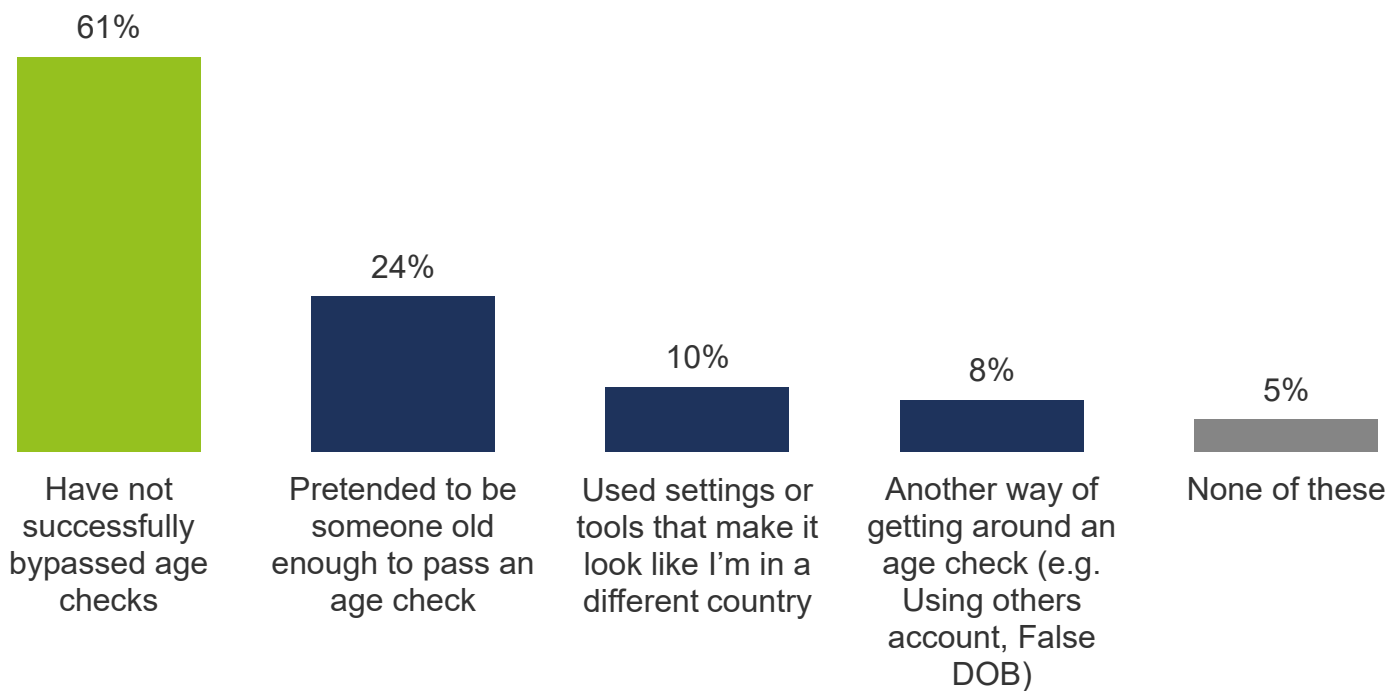
Pretending to be older is the most common way of getting around age checks although some use location-changing tools

When children attempt to bypass an age check, the methods they use vary. Among those who have bypassed, 63% said they had pretended to be someone else (24% of all children), 27% said they have used settings or tools that make it look as though they are in a different country. This accounts for 10% of all children saying they have used settings or tools that make it look as though they are in a different country to bypass age checks.¹² This wording was used to capture those who had used a VPN to bypass, while not directing children who had not used a VPN for bypassing age checks on how to do so. 22% said they had used some other method, accounting for 8% of all children.

¹² 4% of children chose this answer despite not saying they had ever used a VPN at a previous question. This could be due to question wording at this stage highlighting that their individual answers would not be shared with anyone. This group is not included in the analysis on those saying they have used VPNs in the last three months but were still asked follow up questions on VPN use.



Figure 22: Methods of bypassing age checks among all children



Source: D03. "Have you done any of the following to get past age checks and access features, apps, platforms or websites that you're too young to use?" Base: all respondents (n=2,299)

Using settings or tools was concentrated in older children

Only 6% of all 11- to 12-year-olds indicated that they had used settings or tools to make it look like they were in a different country, compared with 13% of 13- to 15-year-olds and 11% of 16- to 17-year-olds. 14% of those with impacting/limiting conditions also indicated they had done this. Usage is highest among children who indicated they had used a VPN in their lifetime, at 25%.

Open text responses for settings or tools suggests many are using VPNs

In a follow up open question, respondents were asked, if they felt comfortable, to say how they got round age checks. Although a large number chose not to divulge an answer, among those who gave an answer 60% indicated they had used a VPN, while 17% indicated they had changed their device / application region settings.

Children who pretended to be someone old enough to pass an age check most commonly indicated their method of getting round age checks was a false date of birth (45%) linked with self-declaration checks, although a notable minority also said they had used their parents or relatives identification details (11%), or used someone else's identification (5%) while 6% said they had used altered images or disguises to appear older.

Location-changing tools are most often used to reach gaming and adult content

The reasons children gave for their most recent use of bypass methods reflect differences in the types of content they were trying to access. Children who used settings or tools that made it look



like they were in a different country did so for a fairly even spread of purposes, led jointly by online gaming (35%) and accessing adult content (e.g. 18+ rated or violent content) (35%), and followed closely by accessing restricted features such as live streaming (34%) and chat or messaging apps (33%).

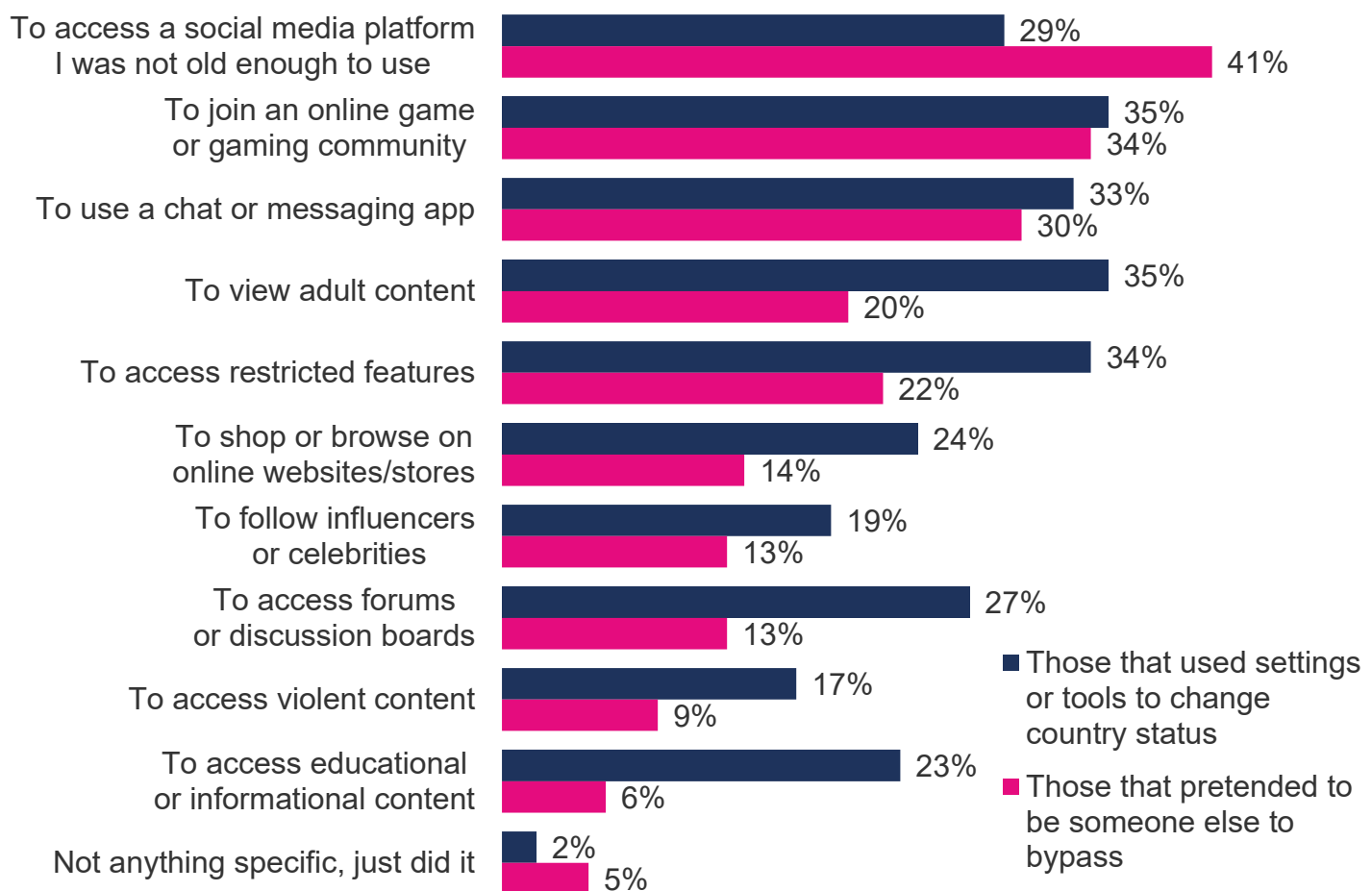
Those who pretended to be someone else to bypass age checks were most likely to use it for accessing social media platforms they were too young for (41%), to join an online game or gaming community (34%) or to use a chat or messaging app (30%).

Certain types of content were more likely to be accessed by those who used settings or tools over those who pretended to be someone else to bypass age checks. Accessing educational or informational content was cited by 23% of those who used settings or tools to bypass vs. 6% among those who pretended to be someone else. Accessing adult content was cited by 35% of those who used settings or tools compared with 20% of those who pretended to be someone else.

Types of content accessed also vary between groups. Children who have used a VPN in the past 3 months are consistently more likely to be accessing adult content, and this holds for both those who said they had used settings or tools to change country status (45%), and those who said they had pretended to be someone else to bypass age checks (32%).



Figure 23: Reasons for bypassing age checks



Source: D04. "What were you trying to do?" Base: all those that used settings or tools to change country status (n=272), pretended to be someone else (n=582)

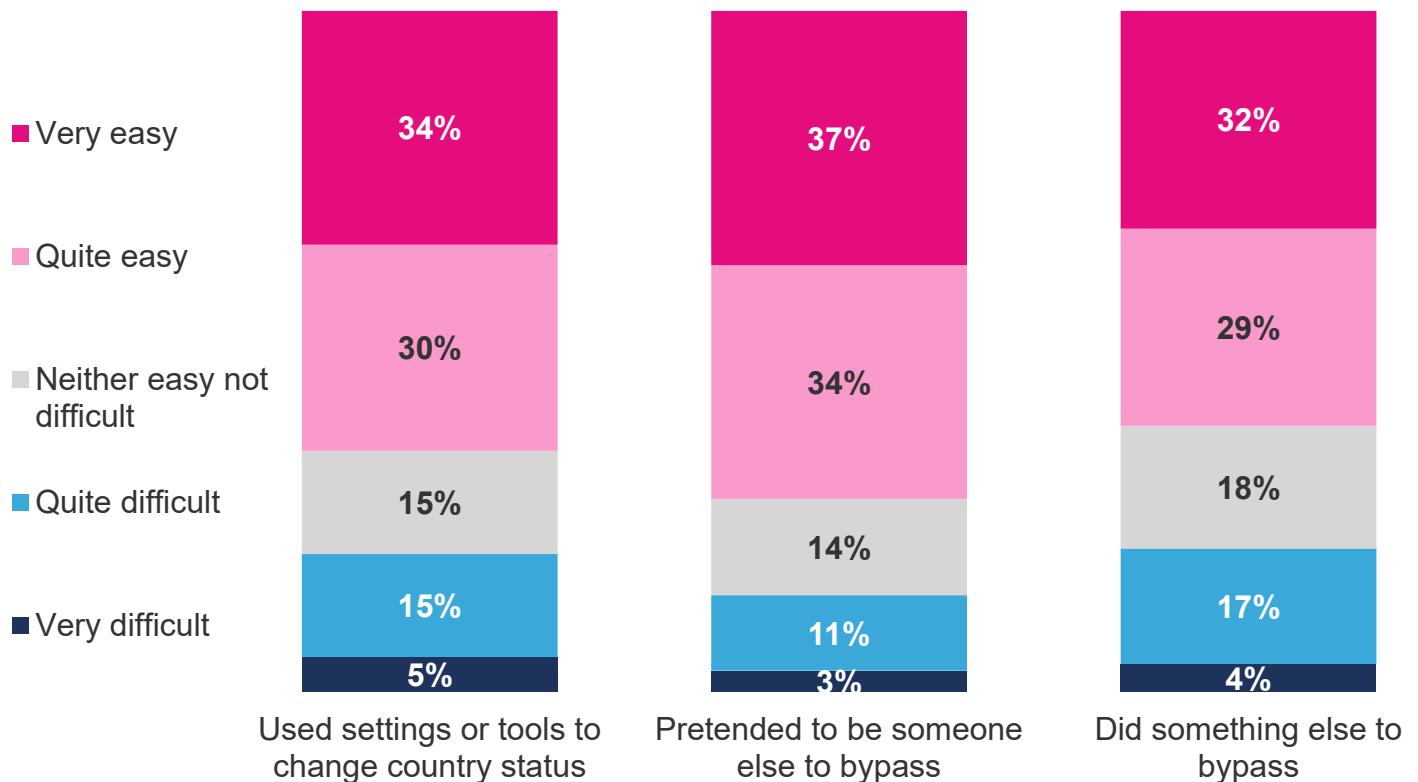
Most children who get around checks find their method of circumvention easy

Among children who have bypassed age checks, a clear majority found the methods they used easy.

71% of those who pretended to be someone else who was older said it was easy to bypass age checks, while 64% of those who used settings or tools to make it look like they're in a different country and 61% of those who used another method said it was easy to get around age checks using that method.



Figure 24: Perceived ease of bypass methods



Source: D06. "Thinking about the most recent time you ... how easy or difficult was it to get around the age check?"
 Base: all those that used settings or tools to change country status (n=272), pretended to be someone else (n=582), did something else to bypass age checks (n=215)

Children most often learn how to get around age checks from friends

Circumvention is mostly a skill children learn from each other. Of those who have got around an age check, three in five (59%) say they learned how to do so from friends or others their own age. Around a fifth (21%) worked it out for themselves. Online videos such as YouTube, TikTok or Instagram, were the source for learning how to bypass age checks for just under a fifth (18%), while family members collectively account for a quarter (25%), with only one in ten (10%) saying they had learned from a parent or guardian.

The sources of support children reported varied across different groups. Siblings play a much larger role in bigger families. Brothers and sisters were the source for 23% of children in households with four or more children. The same household pattern shows up in circumvention overall, with 54% of children in the largest households having got around a check at all, compared with 35% in single-child homes.

For learning how to bypass age checks, online videos are used more heavily by children from an ethnic minority background (25%, against 16% of white children) and by current VPN users (27%).

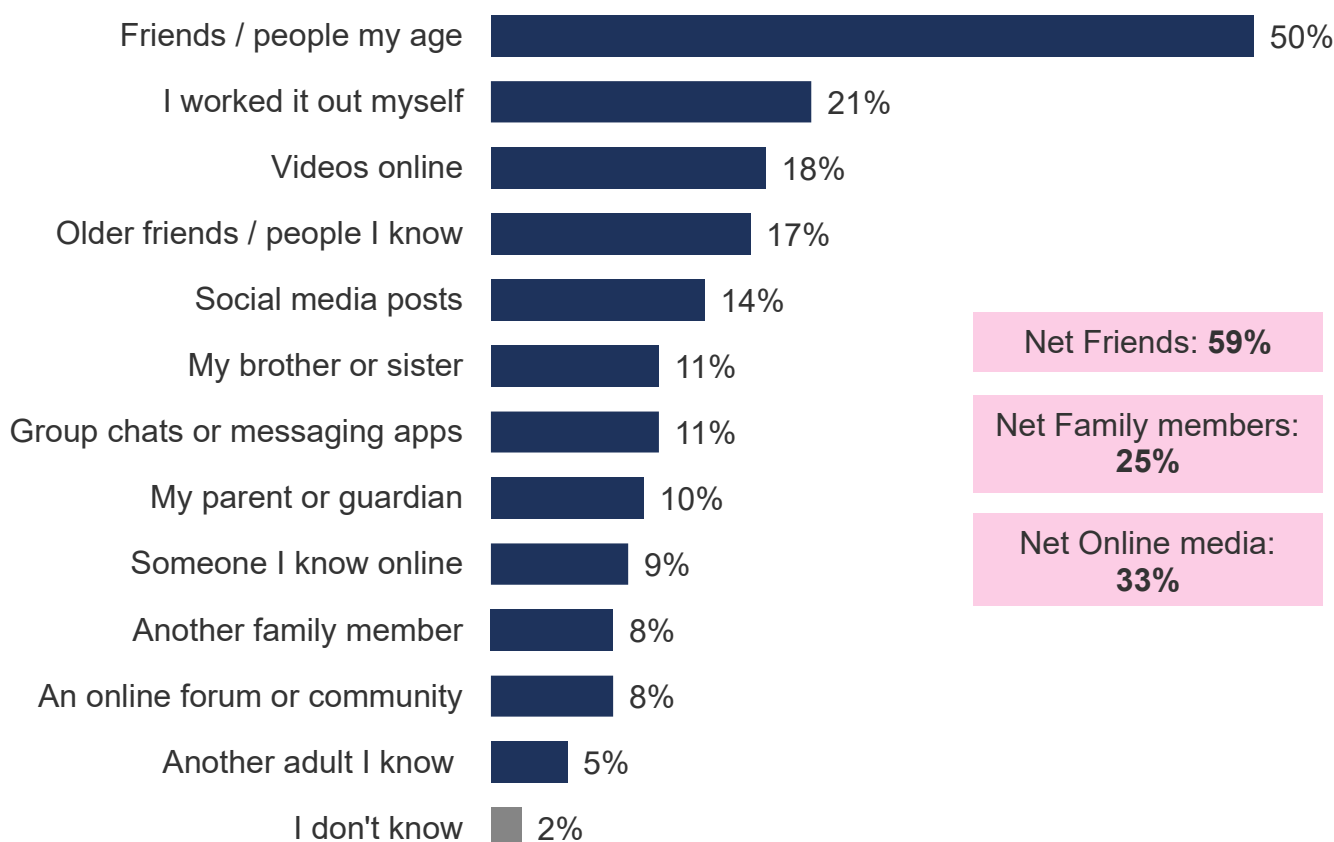
The share of children who say a parent actively helped them get around a check (4% of children in total) is far lower than the share who say a parent had helped set up their VPN, suggesting parents are far more often enabling VPNs than directly helping children with circumvention.

The way children learn also differs according to what they are trying to reach. Those who have got around a check in order to access adult content are more likely than others to have been taught by



older friends (26%), online videos (28%) or social media posts (25%), and are less likely to have simply worked it out for themselves (14%).

Figure 25: How children learn to bypass age checks



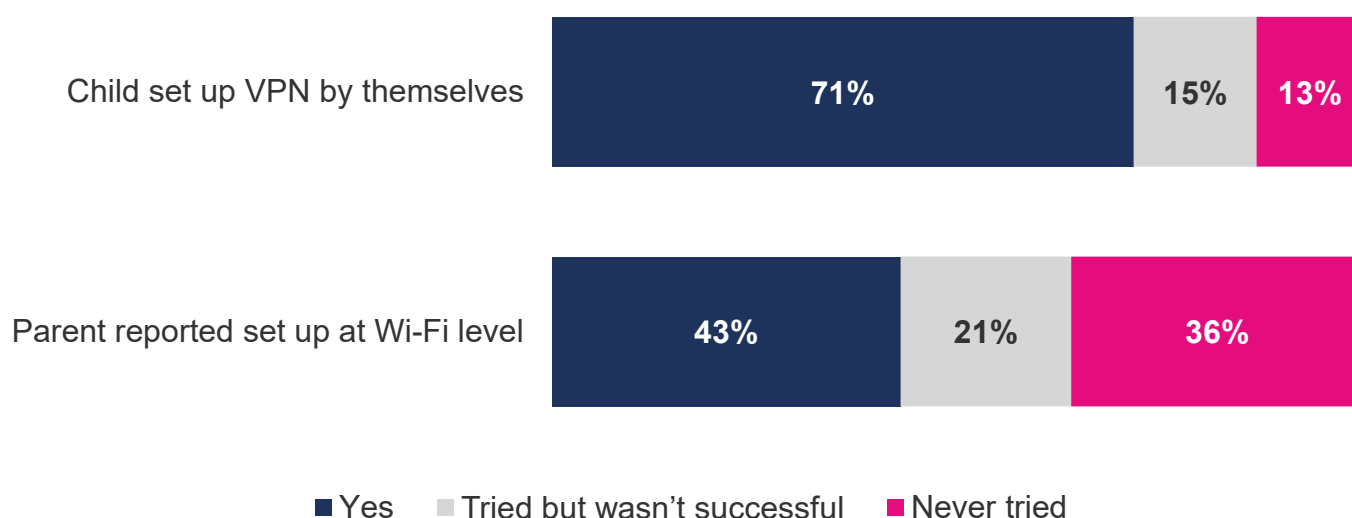
Sources: D09. "Thinking about the ways you have got around age checks in the past, where or who did you find out how to do this from?" Base: all children who have got around age checks (n=823)

Bypassing success varies by how the VPN was set up

Where a VPN has been set up at the Wi-Fi level, children appear less likely to report getting around a check (43% successful) compared to when VPNs are set up on specific devices (53% successful). This may reflect the fact that a network-wide VPN reduces the number of device-level checks children encounter in the first place.



Figure 26: Bypassing success by set up of VPN



Source: D02b Have you ever been successful in getting around age checks (i.e. accessing despite age restrictions)?
Base: Child set up VPN by themselves (n = 325); Children whose parents report setting up a VPN at Wi-Fi level (n= 228).

Some parents are unaware their child has got around a check

When parents were asked whether their child has taken steps to get around an age check, a quarter (25%) of parents said they were aware that their child has succeeded in getting around an age check, while 13% said their children had attempted but not been successful.

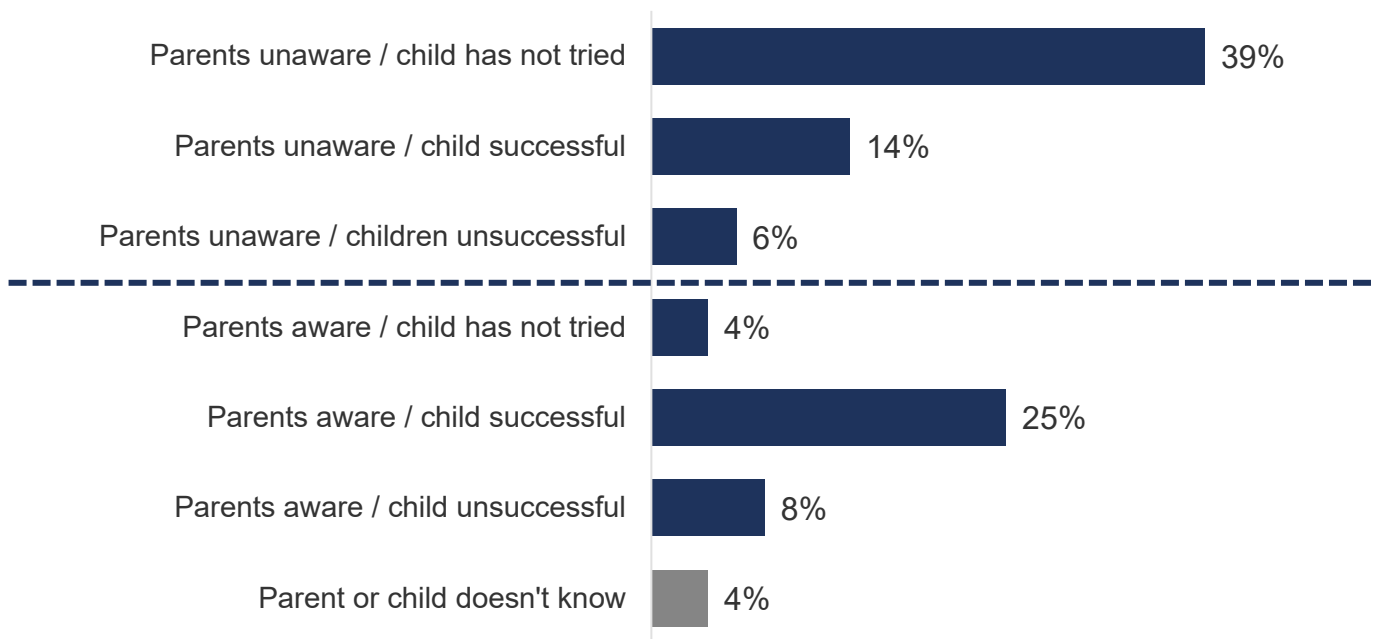
Over two in five (43%) said their children had not attempted to get around any age check, and a fifth (20%) said they did not know. This compares to nearly two in five children (39%) who say they have successfully got around an age check, and a further 14% of children say they tried but were unsuccessful, and 43% say they have never tried.

When these answers are cross-referenced, we find that 14% of parents are unaware their child was successful in getting around an age check, meaning that for a notable minority of children, the behaviour goes undetected at home. This group is more likely to be older children (18% for 16- to 17-year-olds, 16% for 13- to 15-year-olds and 8% for 11- to 12-year-olds) and those who have set up a VPN themselves (24%).

This is consistent with the broader pattern of increasing digital independence among older teenagers who are more likely to set up their own VPNs, use VPNs in households where no parent reports having one, and also to bypass age checks.



Figure 27: Parental awareness of child taking steps to bypass age checks



Source: Combining D02b “Have you ever been successful in getting around age checks (i.e. accessing despite age restrictions)?” / A06. “To your knowledge, has your child taken steps to get around age checks to access online services for which they are under the minimum age?” into combined chart on parental awareness of bypassing Base: all respondents (n=2,299).

Children recognise the risks of getting around age checks

Children who had bypassed age checks generally reported awareness of a range of potential risks. Nearly half (49%) recognise the risk of seeing upsetting content and a similar proportion (45%) cite the risk of talking to strangers.

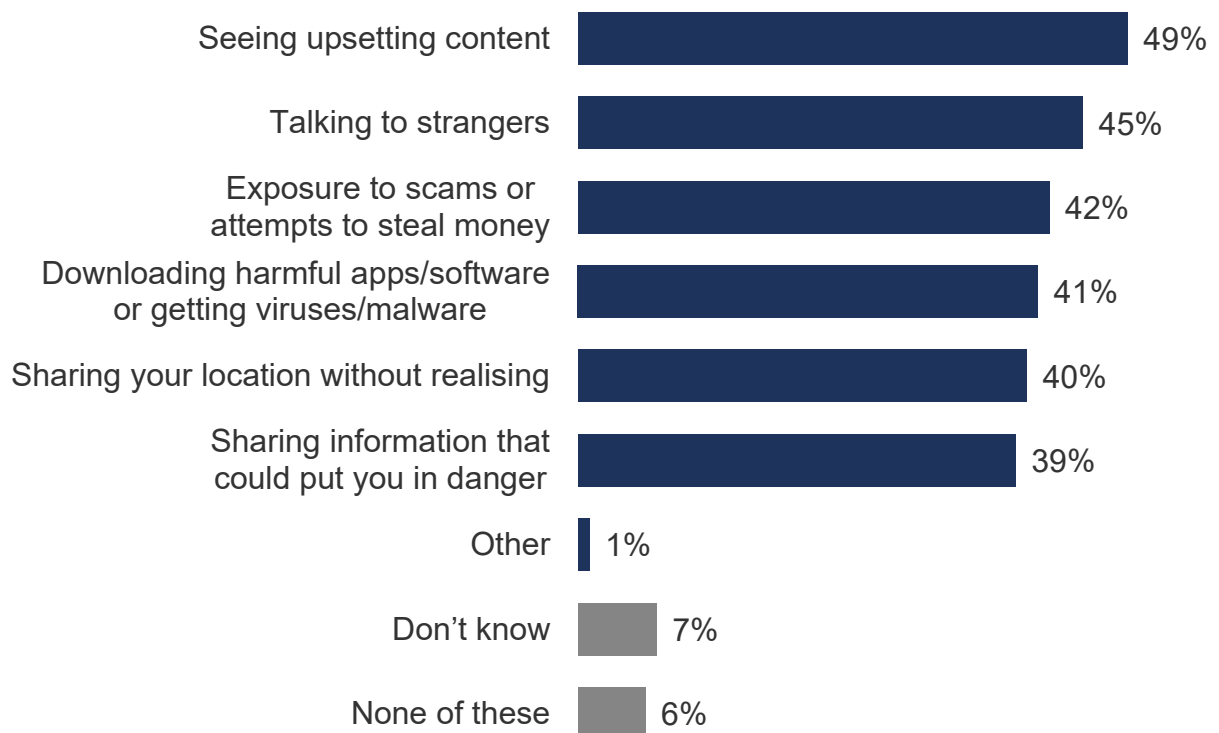
Around four in ten cite exposure to scams (42%), downloading harmful software or viruses (41%), sharing their location without realising (40%) or sharing information that could put them in danger (39%). Only 6% say none of these risks apply to them and 7% say they do not know.

Older children are less likely to identify talking to strangers as a risk (37% of 16- to 17-year-olds) while younger children are less likely to cite downloading harmful apps and getting viruses (32% of 11- to 12-year-olds). These shifts mirror age differences in how children define online privacy, with younger children focused on harm from strangers while older children increasingly refer to data security.

The high level of risk awareness among children who have got around age checks suggests that children are aware of what they may be exposed to in doing so but have chosen to do so anyway.



Figure 28: Perceived risks of bypassing age checks



Source: D11. "Which of the following, if any, do you think might be risks that you could face when getting around age checks?" Base: all children who have got around age checks (n=823)

Practical measures are seen as the strongest deterrents to bypassing

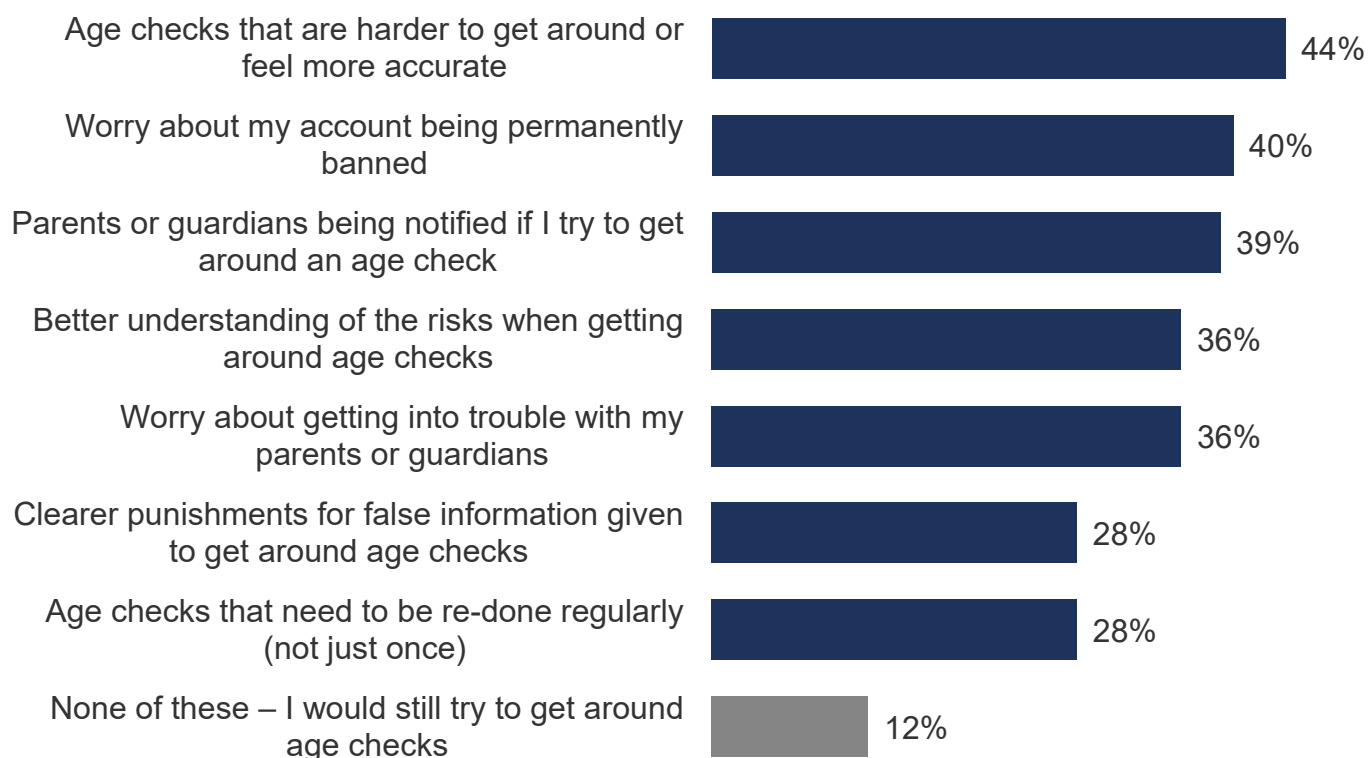
Children say they would be most deterred by measures that make bypassing harder or carry real consequences. The most commonly cited deterrents are age checks that are harder to get around or feel more accurate (44%), worry about an account being permanently banned (40%) and parents being notified if they try (39%).

A better understanding of the risks (36%) and worry about getting into trouble with parents (36%) are also selected by just over a third. 12% say nothing would deter them.

Those who have used a VPN in their life are more likely to say that a better understanding of the risks when getting around age checks would help (42% vs. 32% of non-VPN users), and age checks that need to be re-done regularly, not just once (34% vs. 25% of non-VPN users) would deter them from trying to get around age checks.



Figure 29: Deterrents of bypassing age checks



Source: D12. "What might make you less likely to get around age checks in future?" Base: all children who have got around age checks (n=823)



Section 4: Harms faced online

Over half of children have experienced certain harmful online exposures in the last three months

Just over half of children (53%) say they have seen or interacted with content not meant for them in the last three months.

Among children who were asked about these types of content,¹³ the most commonly reported experiences are seeing violent content (26% of 11- to 17-year-olds), content promoting unrealistic body types (e.g. extremely skinny or muscular) (26% of 13- to 17-year-olds) and hateful content such as racism, homophobia, ableism, transphobia or sexist content (25% of 13- to 17-year-olds).

Just under a sixth report that an adult they don't know has tried to contact them or sent them messages in the past 3 months, or that someone has requested personal or sensitive information from them (14% each).

Almost one in five children aged 13 to 17 have recently seen explicit sexual content or nudity online (17%), and a slightly smaller proportion have seen content about self-harm (13%). Two in five children (43%) report experiencing none of these.

Notably, 7% of 13- to 17-year-olds have used a VPN in the last three months and seen explicit sexual content.

The majority of harmful content is encountered passively

When asked how children came across these harms most recently, most reported coming across it passively while scrolling, rather than deliberately searching for it. This is the dominant route for encountering body image content (74% of those who saw it encountered while scrolling), violent content (66%), hateful content (62%) and self-harm content (57%). Comment sections are a notable secondary route for encountering hateful content, with over a fifth (22%) encountering it this way.

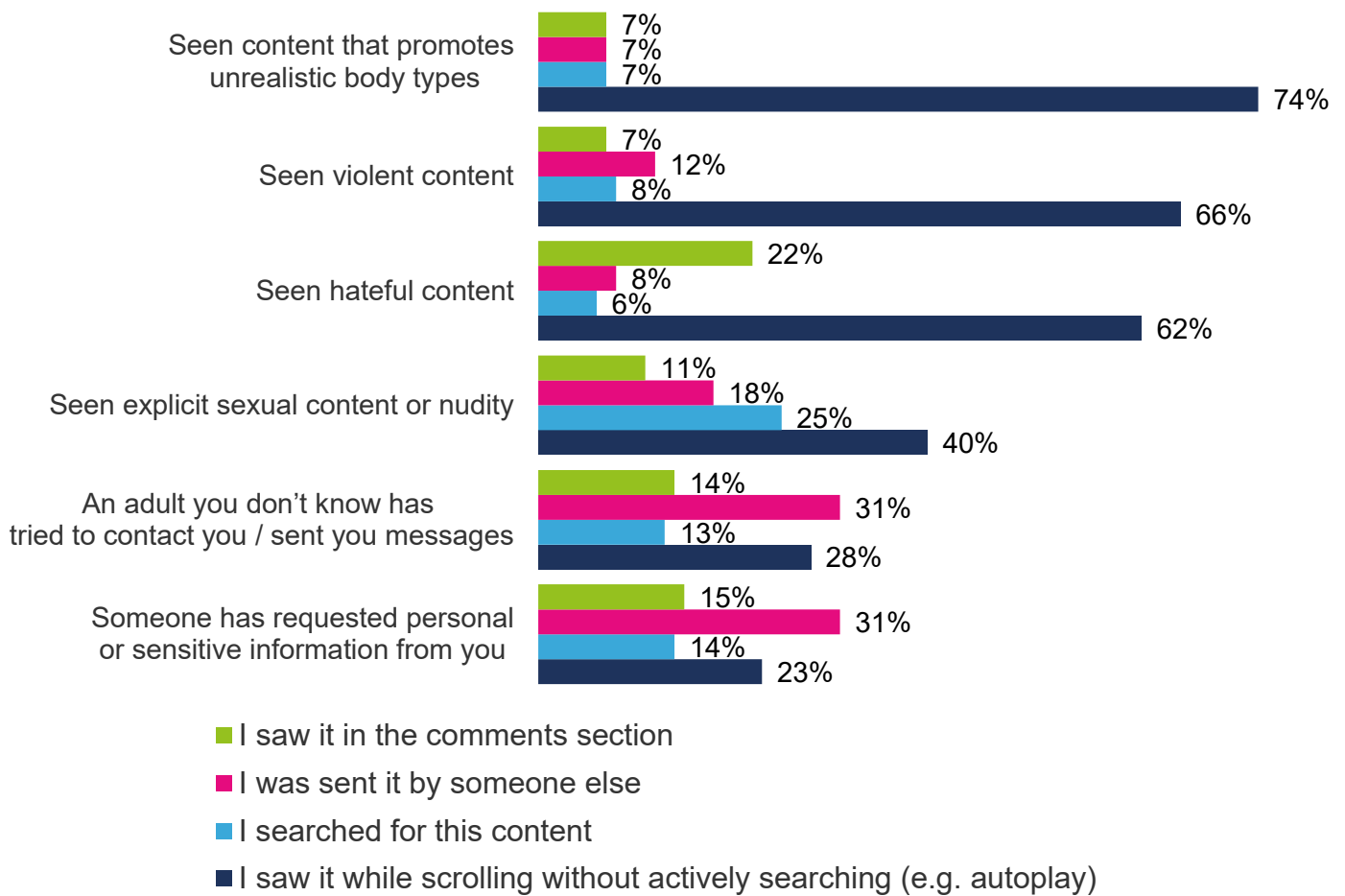
There are important exceptions to this pattern of passive encountering. Explicit sexual content was more likely to have been actively searched for than any other category included: a quarter (25%) of children who saw it had searched for it, far exceeding the search rate for self-harm content (13%), violent content (8%), unrealistic body-image content (7%) and hateful content (6%). Similarly, nearly a fifth (19%) of content encouraging dangerous activity was searched for instead of passively viewed while scrolling.

For contact from unknown adults and requests for personal information, being sent content directly is the most common route, at 31% in each case.

¹³ Certain answer options were only shown to 13+. (Seen explicit sexual content or nudity; seen hateful content; seen content that promotes unrealistic body types; seen content about self-harm).



Figure 30: How harmful content was experienced



Source: F02 “Thinking about the most recent time each of these happened, how did it happen?” Base: Children who had each experience in the last three months (Seen explicit sexual content or nudity n=320; An adult you don’t know has tried to contact you / sent you messages n=349; Someone has requested personal or sensitive information from you n=362; Seen violent content n=642; Seen content that promotes unrealistic body types (e.g. extremely skinny or muscular ones) n=486; Seen hateful content n=474)

Children’s routes to harmful content vary by gender

Boys are significantly more likely than girls to have encountered explicit sexual content through searching (32% compared with 16%), while girls are more likely to have come across it while scrolling (50% compared with 34%).

For self-harm content, girls are significantly more likely to have encountered it passively while scrolling (67% compared with 45% of boys), while boys are more likely to have been sent it directly (18% compared with 7%).

Boys who have seen violent content are also more likely than girls to have been sent it by someone else (16% compared to 8%).



Explicit sexual content shows the strongest association with bypassing age checks

Among children who have got around an age check, around half (51%) reported that they saw at least some harmful content after getting around it. This amounts to 20% of all children having seen harmful content after getting around an age check in the last three months.

Explicit sexual content shows the clearest association with bypassing behaviour, as over a third (35%) of children who bypassed an age check and saw explicit content said they saw it *only* after getting around an age check. This is the highest “only after bypassing” figure for any content type.

A further 45% say they saw it both after getting around an age check and without getting around one. Taken together, eight in ten (80%) children who bypassed and saw explicit sexual content experienced at least some of that content after getting around an age check.

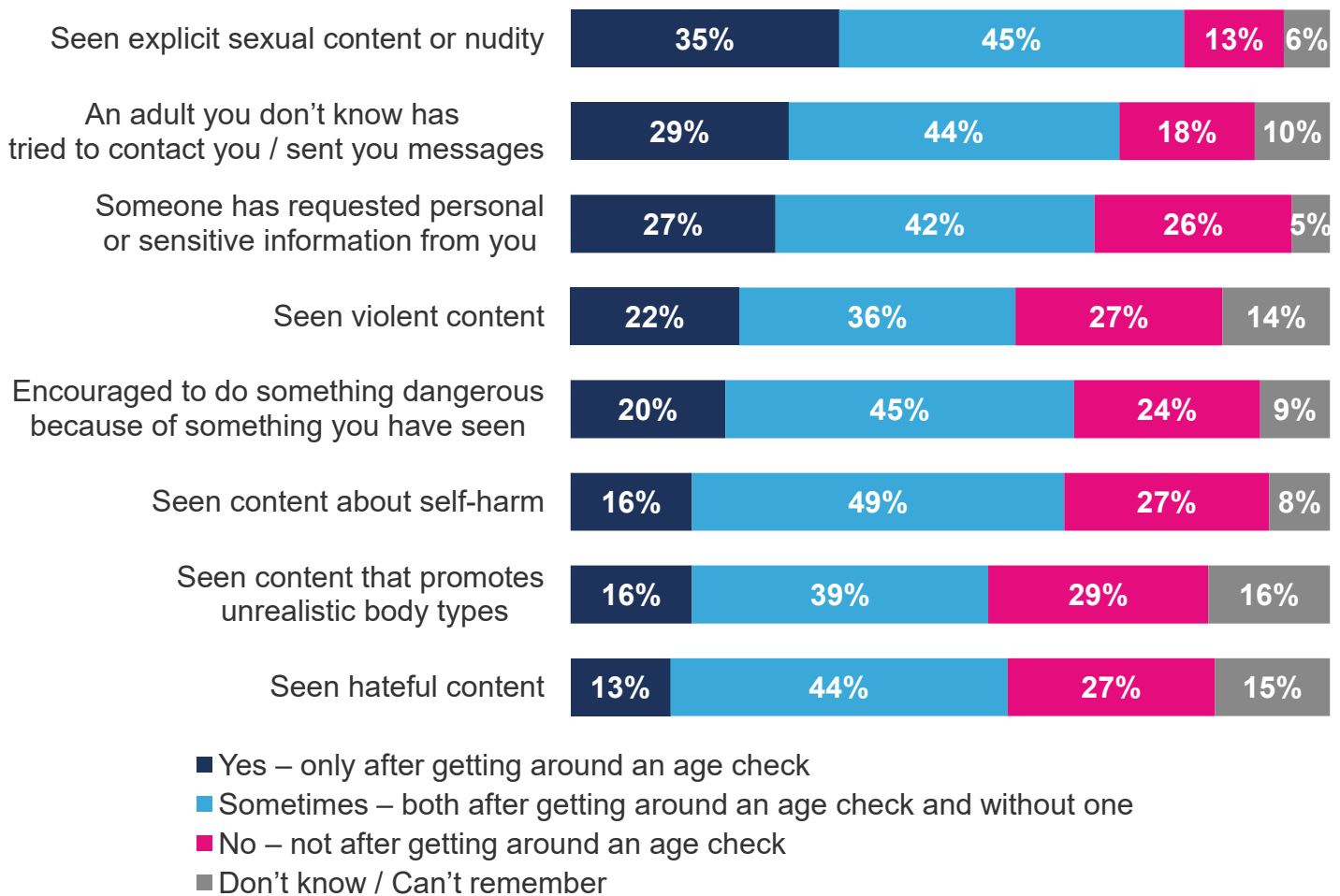
Contact with unknown adults and requests for personal information are among the harms most associated with bypassing age checks

The next most reported association with bypassing age checks was receiving contact from unknown adults. Among those who experienced it in the last three months, 29% say it happened only after getting around a check, and a further 44% say it happened both after bypassing and at other times. Requests for personal information showed a similar pattern, with 27% reporting this happened only after bypassing and 42% saying it occurred both after bypassing and in other contexts.

For other content types, the “only after bypassing” figures are lower. Just over a fifth (22%) of children who got around an age check and saw violent content did so only after bypassing, a similar proportion (20%) for dangerous challenges, 16% for both body image content and self-harm content, and 13% for hateful content, but the “sometimes after bypassing” proportions remain substantial, meaning that for most content types, at least some has occurred after bypassing an age check.



Figure 31: Content most likely to be seen after bypassing an age check



Source: F03. "Did you see it after getting around an age check?" Base: Children who had got around age checks and had each experience in the last three months (Seen explicit sexual content or nudity n=191; An adult you don't know has tried to contact you / sent you messages n=199; Someone has requested personal or sensitive information from you n=206; Seen violent content n=328; Encouraged to do something dangerous because of something you have seen online (e.g. a challenge or dare) n=139; Seen content about self-harm n=146; Seen content that promotes unrealistic body types (e.g. extremely skinny or muscular ones) n=241; Seen hateful content n=246)

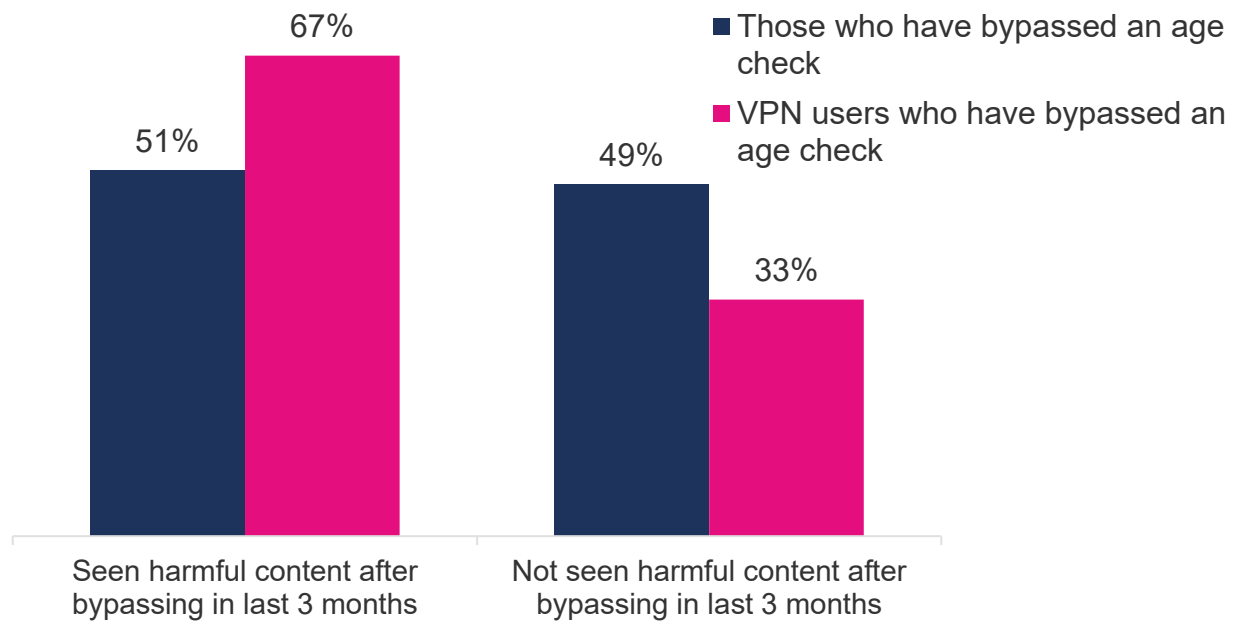
VPN users are more likely to have experienced harmful content than users who have bypassed age checks in other ways

Among children who have both bypassed an age check and currently use a VPN, the likelihood of having seen harmful content after bypassing is significantly higher: 67%, compared with 43% of children who have bypassed but never used a VPN.

Although older children who have bypassed age checks are more likely to have experienced harms directly after bypassing a check than younger children (38% for 11 to 12, compared with 58% of 13 to 15s and 48% of 16 to 17s), and VPN users are likely to be older, that does not explain the full extent of the association between using VPNs and experiencing harmful content after bypassing age checks.



Figure 32: Recent experience of harmful content online in all children and VPN users



Source: F03. "In the past 3 months, when you have seen [content type], did you ever see it after getting around an age check?" Base: all children who have bypassed age checks (n=943), current VPN users who had bypassed age checks (n=375)





www.bmgresearch.com

