

# Internet Matters' response to DSIT's consultation: Growing up in the online world: a national conversation

(May 2026)

## Introduction

The Government consultation '*Growing up in the online world*' comes amidst increasing scrutiny over children's online safety and wellbeing. There is widespread concern that online services are not doing enough to protect children from harm. This has led to growing calls for stronger intervention, including proposals to restrict children's access to social media and other online services.<sup>1</sup>

These concerns are rooted in what many families are experiencing every day. Children are growing up in an increasingly digital world, where technology is embedded in how they learn, socialise, play, create, seek support and access information. Many children benefit from these digital experiences, but many are also telling us that they see upsetting content, struggle to judge whether information is trustworthy, and find it hard to manage the amount of time they spend online. This tension is growing as AI reshapes education, work and everyday life.

That is why the answer cannot simply be to ask whether children should be online, or which services they should be kept away from. The policy question should instead centre on how, in a digital world, we can ensure that the digital services children use are safe, age-appropriate and designed with their wellbeing in mind. This requires a more nuanced approach than blanket bans alone.

Internet Matters welcomes the consultation's focus on the wide range of factors that shape the online experiences children have. Children's safety and wellbeing are not determined only by the content they see but also by how services are designed, what features children can access, who can contact them, how content is recommended, and how easy it is to disengage.

The Online Safety Act is an important starting point for strengthening children's online safety, and our research suggests that some families are seeing the impact of the Act's requirements.<sup>2</sup> However, families also tell us that more action is needed. Parents<sup>i</sup> and children recognise their own role in staying safe online, but they are clear that they cannot do this alone. Government, regulators and industry must all play their part.

---

<sup>i</sup> Throughout this response, we use "parents" as shorthand for parents and carers, including adults with parental responsibility or another caring role in a child's life.

Internet Matters' response to the Government's consultation is grounded in the experiences of children and parents. We draw on research from our [Digital Wellbeing Index](#) and [Internet Matters Pulse](#), and our recent reports on [AI chatbots](#), [children's online news consumption](#), [image-based abuse](#), [gaming](#), [parental controls](#) and [families' experiences under the Online Safety Act](#). All quantitative evidence cited in this response is based on nationally representative research with UK children and parents, carried out with registered polling companies including Opinium Research and BMG Research. In addition to responding to the Government's online survey, we are submitting the below consultation response in order to set out the evidence and reasoning behind our positions in more detail. This document follows the structure of the consultation.

Our central argument is that policy should support children to engage with digital technology safely, positively and in ways that improve their wellbeing, learning and development. This means protecting children from harm, while ensuring they can continue to benefit from the opportunities digital life can provide. Internet Matters recommends that Government take a targeted, risk-based approach to children's online safety, focused on the services, features and design choices that create the greatest risks, over a blanket ban on categories of services for under-16s.

First, all services used by children should be required to demonstrate that their minimum ages, features, defaults and safeguards are appropriate for the children they allow to use them. This means ensuring that age restrictions are meaningful, that children are given age-appropriate experiences, and that safety is built into services from the outset.

Second, Government should restrict children's access to the highest-risk functionalities and ensure age assurance works in practice to do so effectively. This includes features that expose children to harmful contact, image-sharing, livestreaming, location sharing, disappearing content, in-app spending and compulsive use. Age assurance should be used to provide safer, age-appropriate experiences, not only to block access.

Third, Government should strengthen the wider support children and families need to navigate digital life safely and positively. This includes urgent action on AI services accessed by children, stronger media and digital literacy support for families both in and out of school, better access to high-quality online content, and practical support for parents and children with additional needs.<sup>ii</sup> These changes would support families without shifting responsibility away from the

---

<sup>ii</sup> The consultation's definition of additional needs, which covers children who may need extra support for a range of reasons, such as learning, communication, health or access needs, is closely aligned with the definition we take in our research and throughout this document: we define children with additional needs as those who receive Special Educational Needs (SEN) Support, who have a physical or mental health condition that reduces their ability to carry out day-to-day activities, and/or who have an Education, Health and Care Plan (EHCP) or equivalent.

services children use. Government must also effectively communicate any changes to families and support them to ensure effective implementation.

Taken together, these measures would create a safer, healthier and more positive digital environment for children.

## Chapter 1: Understanding how children use technology

Internet Matters' evidence shows that children's online experiences are becoming more complex and polarised. More children are reporting positive experiences online, alongside more negative experiences. Parents report a similarly mixed picture, recognising the role digital technology can play in children's learning, independence, and connection with others, while also reporting concern about children's exposure to harm, difficulty managing time online, and the effects on sleep, concentration and physical activity.

This chapter explores what sits behind that mixed picture. It looks at the benefits children derive from being online, the harms and risks they continue to encounter, emerging challenges such as generative AI and misinformation, and the different ways children experience digital life depending on their needs, vulnerabilities and wider circumstances.

Children and parents see significant value in online spaces. Overall, the evidence suggests that the benefits of being online somewhat outweigh the risks, but only if children are protected from avoidable harm. Government should therefore protect children from harm while ensuring they can continue to benefit from digital technologies. This requires a focus not only on what children see online, but also on how services are designed, how children use them, and how risks and benefits differ across groups of children.

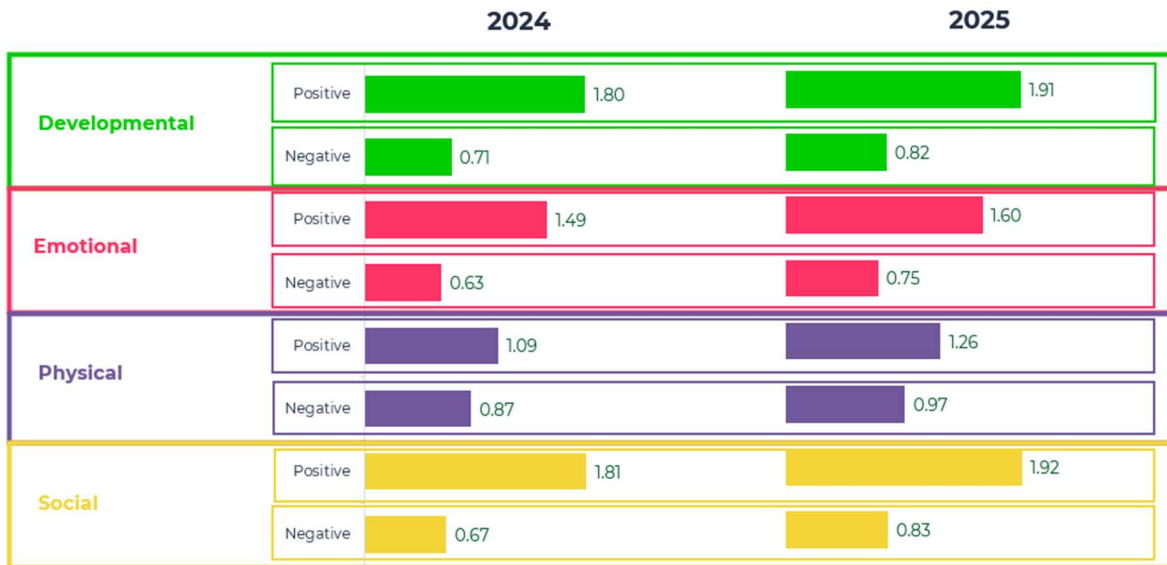
### 1.1 Children's online experiences are becoming more polarised

Internet Matters' *Digital Wellbeing Index (DWI)*, now in its fifth year, tracks how digital technology affects different aspects of children's wellbeing, based on families' experiences.<sup>iii</sup> The *DWI Year 5* shows that children's online experiences are becoming more polarised. Both children's positive and negative digital wellbeing scores increased in 2025 compared to previous years, meaning more children are reporting positive experiences online, alongside reporting more negative experiences (Figure 1).<sup>3</sup> This builds on the "internet of extremes" pattern identified in the *DWI Year 4*, where children's positive and negative wellbeing scores first appeared to diverge.<sup>4</sup>

---

<sup>iii</sup> Internet Matters' [Digital Wellbeing Index \(DWI\)](#) is an annual, nationally-representative household survey of over 1,000 UK children and their parents, tracking the impact of digital technology across four dimensions of wellbeing: emotional, social, developmental and physical wellbeing. DWI has been conducted annually since 2021 and was developed by the University of Leicester.

Figure 1. Digital wellbeing index – Index scores for children



**Figure 1. Digital wellbeing index- Index scores for children** | Data from *Children's Wellbeing in a Digital World Year 5 (2026)*.  
 Base: All children 2024 (1,054) 2025 (1,270)  
 Indexes calculated through combination of answers throughout children's questions  
 Boxes indicate a significant increase in the score between 2024 and 2025

The *DWI* also includes a parent index, which measures parents' perceptions of how digital technology affects different aspects of their child's wellbeing. In the *DWI Year 5*, parents' scores increased across both positive and negative dimensions of children's digital wellbeing.<sup>5</sup> This suggests that parents are also seeing children's digital lives become more polarised: they are reporting stronger positive impacts from digital technology, but also stronger negative impacts.

This polarisation matters because children's online experiences are rarely neatly positive or negative. The same activity can support children's wellbeing in one respect while creating risks in another.

Children's engagement with news on social media illustrates this clearly. Internet Matters' report *Informed or Overwhelmed?* finds that 74% of children agree that social media helps them feel informed about current events, and 67% say it is where they learn about breaking news. At the same time, 61% of children who consume news on social media report seeing a story that worried or upset them in the previous month, including content relating to war and conflict, violence and death, and crisis events.<sup>iv</sup> This exposure is often unintentional: 40% of children who get news from social media do not follow news-focused accounts, with many encountering news through recommender feeds.<sup>6</sup>

This shows why children's digital wellbeing cannot be understood only by looking at the type of content they encounter. It also depends on how services organise,

<sup>iv</sup> As the survey was conducted July 2025, the 'previous month' refers to the period before this.

recommend and surface that content, and whether children feel able to understand, manage or step away from what they see.

## 1.2 How children benefit from the online world

Digital technologies provide important benefits for children across multiple aspects of their wellbeing. Many children report using the online world to maintain relationships, explore interests and support their learning and development. Internet Matters' evidence suggests that these positive experiences are becoming more common over time.

For example, the *DWI Year 5* finds that 83% of children report that being online is important for staying in contact with friends and family, up from 77% in 2022. Meanwhile 74% say being online helps them find new hobbies and interests, up from 63% in 2022, and 75% of children say being online helps them think about what they would like to do in the future, up from 67% in 2022.<sup>7</sup>

*"You can easily express yourself [on social media] and also get inspiration. [...] I love fashion. I love to see what people think would look good on them." (Girl, 15)<sup>8</sup>*

*"I do a lot of scout camps where I meet lots of new people, and I make loads of new friends. One of the ways that I've been able to keep in touch with those people is through social media." (Girl, 14)<sup>9</sup>*

*"Lots of people use [Discord and Snapchat] to talk to people from all over the world." (Boy, 15)<sup>10</sup>*

Parents also recognise the developmental and emotional benefits of digital technology. For example, 78% of parents report that digital devices and being online have allowed their child to see things or people that inspire them to try new things, up from 73% in 2022, and 75% say the digital world enables their child to discover and pursue interests and hobbies that make them happy, up from 68% in 2022.<sup>11</sup>

Parents also see digital technology as supporting children's social connection and participation. More parents report that being online is very important for their child's ability to stay in contact with people who are important to them, at 45% reporting this in 2025 compared to 30% in 2022. They also report that being online has allowed their child to feel part of a group that they otherwise would not have, with 67% in 2025 compared to 60% in 2022. This reflects the reality that, for many children, online spaces are not separate from their "real" lives, but are part of how they socialise and participate.<sup>12</sup>

These benefits are also visible in children's use of newer technologies. Internet Matters' report *Me, Myself & AI* finds that AI chatbots can support children's learning, exploration and play. Some of the most common reasons children give for using AI chatbots are schoolwork (42%), finding information or learning about something new (40%), curiosity (40%) and fun or escapism (24%).<sup>13</sup>

These findings show that digital environments can play a meaningful role in children's wellbeing. They help children maintain relationships, explore interests, learn, create and imagine their futures. The policy challenge is therefore not simply to reduce children's time online or restrict access to digital services, but to ensure that children can access these benefits in safer, age-appropriate environments.

### 1.3 The risks and harms of children's online experiences

While children report many benefits from the online world, their exposure to harm online remains widespread and persistent. *Internet Matters Pulse*<sup>v</sup> shows that 75% of children report experiencing harm online.<sup>14</sup> This figure has remained broadly stable since 2022. This continued prevalence of harm is one of the reasons further action is needed to protect children online.

Some of the most prevalent harms experienced by children relate to the content they encounter. *Internet Matters Pulse* finds that 22% of children report coming across content which promotes dangerous stunts or challenges, of whom 24% said it caused them high levels of distress, upset or harm. 21% of children report coming across hate speech, of whom 38% said it caused them high levels of distress, upset or harm.<sup>15</sup>

Children also experience harm through their interactions with others online. *Internet Matters Pulse* finds that 15% of children report online bullying, trolling or abuse from people they don't know and 10% of children been asked to give away personal information online.<sup>16</sup> These forms of contact-based harm highlight that risks online are not limited to what children see, but also who they engage with and how those interactions unfold.

Spending too much time online is one of the most reported harms among children in *Internet Matters Pulse*: 44% of children say they feel they spend too much time online.<sup>17</sup> Time spent online is not inherently harmful, but this finding reflects children's own perceptions of difficulty managing their use and the potential for online activity to displace other aspects of their lives. We explore this issue in more detail in Chapter 2.

Parents' concerns broadly reflect the harms children report online. *Internet Matters Pulse* finds that parents' top concerns include children being exposed to misinformation (78%), spending too much time online (76%), contact from strangers (75%) and exposure to violent content (75%).<sup>18</sup>

---

<sup>v</sup> *Internet Matters Pulse* is a bi-annual survey of 1,000 children aged 9-17 and 2,000 parents of children aged 3-17 which tracks a range of topics including children's digital habits, their experience of online harm and parents' perspectives on online safety. An interactive website exploring select insights from *Internet Matters Pulse* can be found here: <https://www.internetmatters.org/pulse/>. N.B. Not all data from *Pulse* contained in this survey is published.

Children's negative experiences are also reflected in how safe they feel online. While a majority of children (72%) reported feeling safe online in 2025, the *DWI Year 5* finds that this has declined from 81% in 2023. This is also more pronounced among children with additional needs who are less likely to report feeling safe online than their peers without additional needs, at 67% compared with 75%.<sup>vi</sup> This suggests that children with additional needs may experience the online world as less safe, alongside facing higher levels of reported harm.<sup>19</sup>

The Online Safety Act and associated Protection of Children Codes, which came into force in July 2025, are intended to reduce children's exposure to online harm. As the regime continues to be implemented, it will be important to monitor whether these measures are changing children and families' lived experience. However, monitoring impact will not be enough on its own. Government must also ensure that the Act remains future-proof, as emerging technologies, including generative AI, are already reshaping the content children encounter and the tools they use, creating new risks and intensifying existing ones.

#### 1.4 Emerging risks in a changing digital environment

New and emerging technologies are adding to the range of risks families need to navigate. Generative AI is a clear example. It is changing both the information children encounter online and the tools they use to seek information, advice and support. This can make it harder for children to judge what is real, trustworthy or generated by AI, while also blurring the boundaries between human and artificial interaction.

One area of concern is the growing challenge of AI-generated content and misinformation. Internet Matters' report *Informed or Overwhelmed?* finds that over a quarter (27%) of children report having believed a fake or AI-generated story, and 41% say they think they may have. Exposure to such content can leave children feeling confused (30%), embarrassed (10%) and less trusting of the news (31%).<sup>20</sup>

Children also recognise the wider social impact of fake, misleading and AI-generated content. 60% say they are concerned about the impact of AI-generated or manipulated content on election results, while 60% say they are similarly concerned about the impact of misinformation on election results.<sup>21</sup> This suggests that children are not only encountering misinformation and AI-generated content in their own online lives, but are also aware of how it can affect trust in information and democratic processes more broadly.

Parents are also concerned about the online information environment. Mis- and disinformation is now one of parents' top concerns about their child's online life,

---

<sup>vi</sup> We define children with additional needs as children who receive special educational needs (SEN) support, who have an Education, Health and Care Plan (EHCP), and/or who have a physical/mental health condition which requires professional help.

sitting alongside more established concerns such as contact from strangers and spending too much time online.<sup>22</sup> This suggests that emerging risks are adding to the range of issues families are trying to navigate.

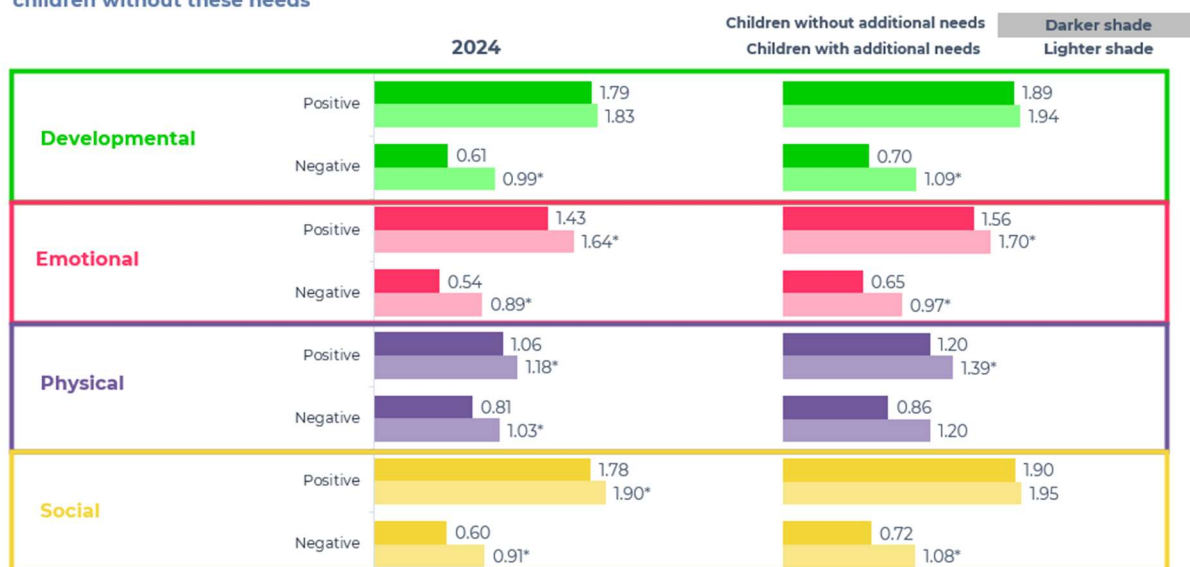
A second area of concern with generative AI is children’s use of AI chatbots. These tools create distinct risks because they are interactive, personalised and conversational. Internet Matters’ *Me, Myself and AI* identifies concerns around children’s over-reliance on AI chatbots and blurred boundaries between human and artificial relationships.<sup>23</sup> We explore the benefits and risks of AI chatbots further in Chapter 2.

### 1.5 Children experience the online world differently

The benefits and harms discussed above are not experienced evenly by all children. Children’s online experiences are shaped by their individual characteristics, needs, vulnerabilities and wider social contexts. Internet Matters’ evidence shows this clearly in relation to children with additional needs, who often experience the digital world more intensely, and in relation to gender, which can affect the types of harms children encounter and how those harms affect them.

The *DWI Year 5* shows that children with additional needs experience more of the good and bad of online life compared to their peers. As shown in Figure 2, children with additional needs have higher positive and negative wellbeing index scores than their peers across all areas of digital wellbeing.

**Figure 2. Digital wellbeing index – Index scores for children with additional needs compared to children without these needs**



**Figure 2. Digital wellbeing index- Index scores for children with additional needs compared to children without these needs** | Data from [Children’s Wellbeing in a Digital World Year 5 \(2026\)](#).

Base: Children without additional needs 2024 (793) 2025 (840); children with additional needs 2024 (246) 2025 (421)  
Indexes calculated through combination of answers throughout children’s questions

Internet Matters' research on neurodivergent children's experiences of online gaming provides a clear example of how some children can benefit from digital spaces in ways that may be particularly important to them. The research found that gaming can provide important benefits for neurodivergent children, including relaxation, entertainment and emotional regulation. Two in five neurodivergent children say playing games on devices helps them stay entertained (44%) and relax (42%).<sup>24</sup> This shows why online spaces can be especially valuable for some children: they may provide downtime, enjoyment and a way to manage emotions, as well as opportunities for connection and learning.

At the same time, children with additional needs are more likely to experience harm. The *DWI Year 5* finds that 79% report experiencing at least one type of online harm, compared to 63% of children without additional needs.<sup>25</sup> The *DWI Year 5* also finds that children with additional needs are more frequently experiencing upsetting interactions with others online, including bullying (27% report experiencing this 'quite a lot' or 'all the time', compared to 12% of children without additional needs). They are also disengaging from positive offline activities, with 30% reporting that they turn down opportunities to meet friends in order to stay online (c.f. 15% of children without additional needs), and 48% avoiding certain apps, websites or games due to negative interactions (c.f. 27%).<sup>26</sup>

These patterns suggest that children with additional needs may require more tailored support, because they are both more likely to benefit from online spaces and more likely to experience harm within them.

Gender also shapes children's experiences of harm. Boys and girls may report similar overall levels of exposure, but they do not necessarily encounter the same harms or experience them in the same way. For example, girls are more likely to see content promoting unrealistic body types (27% compared to 20% of boys), while boys are more likely to encounter explicit sexual content (16% compared to 8%). However, girls are significantly more likely to report feeling upset by harmful content, including explicit material (50% compared to 26%), violent content (67% compared to 53%), and discriminatory content (67% compared to 43%).<sup>27</sup>

These findings show why policy responses must avoid assuming that all children face the same risks or need the same forms of support. A universal approach may leave some children less protected, particularly those who face higher levels of harm, experience harms more acutely, or rely more heavily on online spaces for connection, confidence, learning or support.

## 1.6 What Government must do

The evidence in this chapter shows that children's online experiences are complex. Digital technologies can support children's learning, connection,

creativity and access to support, while also exposing them to harm, pressure and risks that are shaped by service design, how children use services and their individual circumstances. Government should therefore build a balanced, evidence-led response that protects children from harm while preserving the benefits they derive from digital life.

Government should focus on:

- **Protecting children from harm without cutting them off from the benefits of digital life.** Policy should reduce children's exposure to harm while supporting access to the connection, learning, creativity and support that digital technologies can provide.
- **Looking beyond policy that targets content alone.** Children's experiences are shaped not only by what they see online, but by how services are designed, how content is recommended, what features they can access, who can contact them, and how easy it is to disengage.
- **Recognising that children experience the online world differently.** Children with additional needs, vulnerabilities, demographics or different social contexts may face higher risks, experience harms more acutely, or need more tailored forms of support.

These principles inform the more specific policy measures set out in the following chapters: risk-based access to services, restrictions on features that pose risks to children, effective age assurance, media literacy and support for families.

## Chapter 2: Interventions for safer, more positive experiences

Children should be able to benefit from digital services in ways that are safe and appropriate for their age and stage of development. For this reason, Internet Matters does not support a blanket legal ban on children's access to social media. A blanket ban could cut children off from spaces they use for learning, creativity, connection and support, while missing similar risks on other services.

Instead, Government should develop a more targeted, risk-based approach to children's access to digital services that goes beyond social media. Services should be required to show that the children they allow to use them are given safe, age-appropriate experiences. This means looking at the age of child users, the features they can access, the default settings they are given, and whether safeguards are effective in practice.

This chapter argues that Government should set clearer expectations for when minimum ages are needed; require services to enforce age limits effectively; restrict children's access to the highest-risk features; and address design features that encourage prolonged or compulsive use. These requirements should be applied urgently to AI chatbots accessed by children, given the specific risks they create.

### 2.1 Banning children from social media in isolation is not the solution to keeping children safe online

Calls to ban children from social media reflect serious concerns about children's online safety. Many families feel that online services have not done enough to protect children from harm, and that stronger intervention is needed. However, a legally enforced blanket ban on children's access to social media is not the right solution.

Children use a wide range of online services in different ways. The risks they face depend not only on the service they use, but on what that service allows them to do, how it is designed, and the safeguards services put in place to protect children. A blanket ban on social media may appear clear and decisive, but it could miss other services where children face similar risks. It could also prevent children from benefiting from online spaces they use for learning, creativity, connection and support.

#### 2.1.1 A blanket ban would be difficult to define and apply

A blanket ban on "social media" would be difficult to apply because there is no agreed definition of social media. Many online services now combine features such as user profiles, messaging, content sharing, personalised feeds and user-generated content. These features can appear across messaging services, video-sharing platforms, gaming platforms, forums, livestreaming services and AI chatbots. Any ban would require Government to decide which services are

included, which are excluded, and how to respond when services add, remove or change features. A narrow definition could miss services where children face similar risks, while a broad definition could capture services that may be lower risk or more age appropriate.

Australia's under-16 social media restrictions illustrate this challenge. The Australian eSafety Commissioner has identified services including Facebook, Instagram, Snapchat and Twitch as age-restricted platforms.<sup>28</sup> Twitch was added to the list less than three weeks before the restrictions came into force, after the Commissioner assessed that Twitch's livestreaming and interaction features meant it met the criteria.<sup>29</sup> However, other services with significant social or interactive functionalities, such as Discord and Roblox, have not currently been treated in the same way. This shows how quickly boundary questions can arise in practice, and why a fixed category of "social media" can be difficult to apply.<sup>vii</sup> As discussed later in this chapter, services outside such a list may still pose comparable risks to children where they include similar functionalities.

### 2.1.2 Parents support different minimum ages for different services

Parents' views also suggest that a single ban would not reflect how families think about children's online lives. *Internet Matters Pulse* shows that parents select different minimum ages for different services and platforms, rather than applying the same threshold across all interactive online spaces (Figure 3).

Parents do not suggest the same minimum age for every service. They support higher average minimum ages for Instagram, TikTok, Snapchat and X, at around 15 years old, compared with lower average minimum ages for WhatsApp and YouTube, at 14.2 years old. Parents also selected slightly lower average minimum ages for some gaming platforms and networks, including Roblox (13.9), Minecraft (13.8), Fortnite (14.1) and online gaming networks such as Xbox Live, PlayStation Network or Nintendo Switch Online (14.1).<sup>30</sup>

This does not mean gaming platforms or online gaming networks are risk-free. Many include features that can expose children to risk, including messaging, voice chat, in-game purchases, livestreaming and interaction with unknown users. Rather, the data shows that parents distinguish between services when considering appropriate minimum ages, even where those services share similar interactive features. This supports a more targeted approach that looks at what

---

<sup>vii</sup> Australia's regime applies to services that meet the definition of an "age-restricted social media platform". Broadly, this includes services whose sole or significant purpose is enabling online social interaction between users, and which allow users to link to or interact with other users and post material. The regime excludes services whose sole or primary purpose is messaging, online gaming, education, health, professional networking, or photo/video storage. This means services with overlapping social, entertainment, gaming or messaging functionalities may raise boundary questions about whether they meet the criteria.

children can do on a service, and what safeguards are in place, rather than applying a single minimum age across all interactive online spaces.

**Figure 3. Parents views on age of access for popular social media and gaming platforms**

Platform or app	Average minimum age supported by parents (in years)*	% of parents: there should be no restrictions	% of parents: no child should have access to this platform
Instagram	15.0	1%	9%
TikTok	14.9	1%	11%
Snapchat	14.9	1%	12%
X	15.2	1%	16%
WhatsApp	14.2	2%	4%
YouTube (excl. YouTube Kids)	14.2	3%	5%
Roblox	13.9	3%	4%
Minecraft	13.8	3%	3%
Fortnite	14.1	4%	3%
Online gaming networks e.g. Xbox Live, PlayStation Network	14.1	3%	5%

**Figure 3. Parents views on age of access for popular social media and gaming platforms** | Data from [Internet Matters Pulse](#) (May 2026)

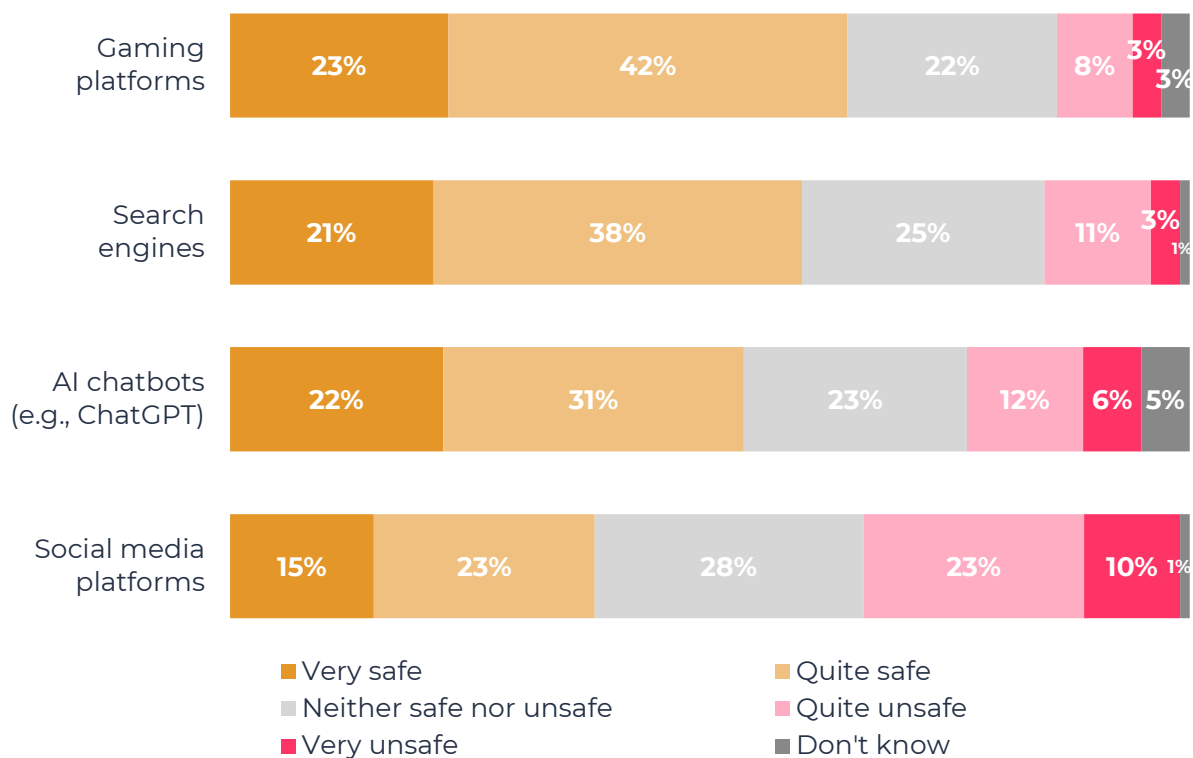
Base: All parents (2000). Q: What do you think the minimum age should be for children to use each of the following popular social media platforms / popular gaming platforms and networks?

\*Alternate base: Floating bases of those parents who agree with some form of minimum age restriction for different platforms

### 2.1.3 Parents also distinguish between services when assessing safety

Parents' views on the safety of different online spaces also suggest that they distinguish between online services, rather than treating all as equally risky. Internet Matters' report *The Online Safety Act: Are children safer online?*, finds that parents are less likely to view social media platforms as safe for children than other online spaces (Figure 4). Only 37% of parents view social media platforms as safe, compared with 64% for gaming platforms, 59% for search engines and 53% for AI chatbots. Parents also view social media platforms as the most unsafe spaces (33%) followed by AI chatbots (18%), search engines (14%) and gaming platforms (11%).<sup>31</sup>

**Figure 4. Parents' perceptions of the safety of different online platforms and services**



**Figure 4. Parents' perceptions of the safety of different online platforms and services** | Data from [The Online Safety Act: Are children safer online?](#) (2026)

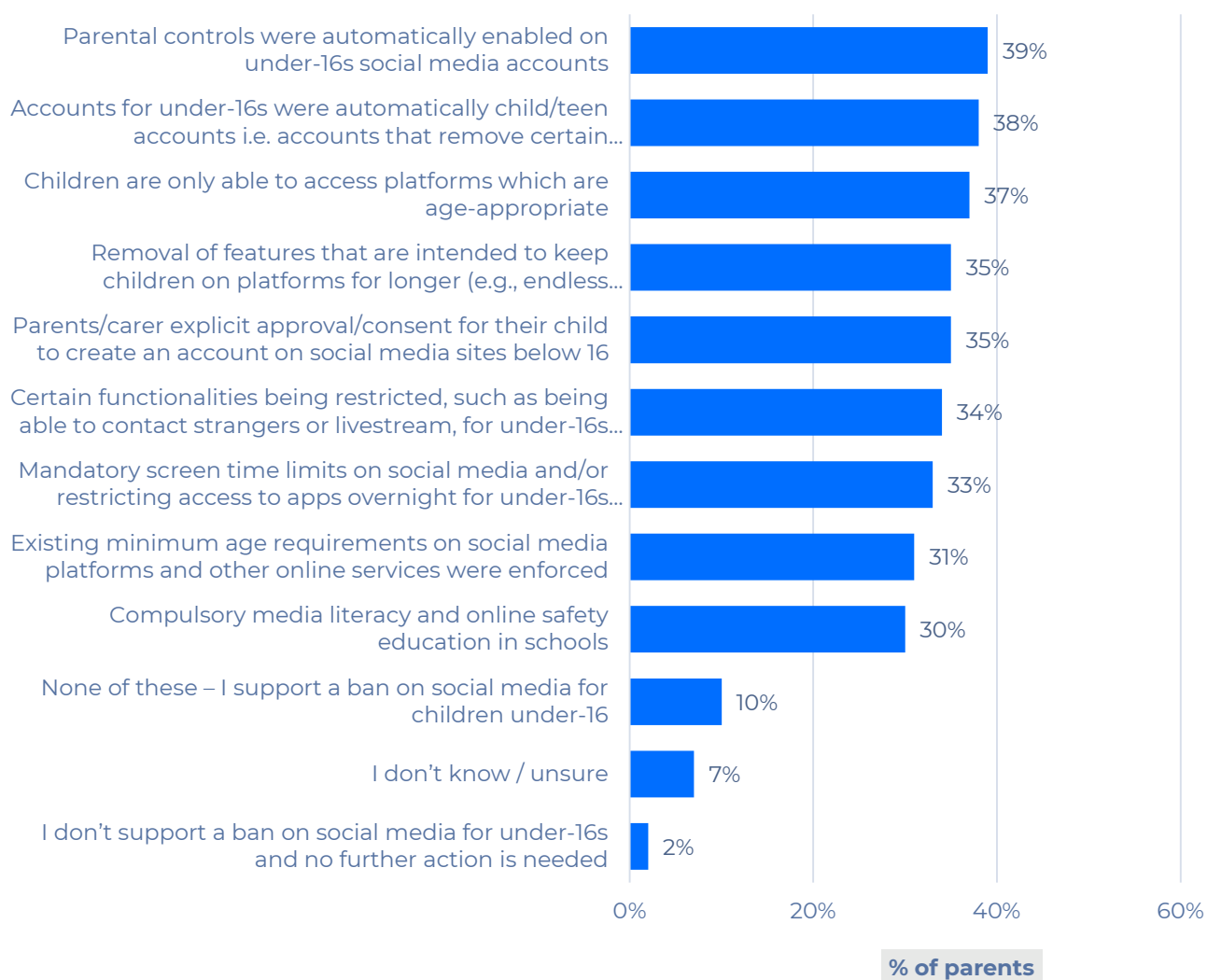
Base: All parents of children 9-16 (1,270). Q: To what extent do you think the following online environments are safe or unsafe for your <age> year old <son/daughter>?

However, parents' perceptions of platform safety should not be the only basis for policy decisions. Some risks may be less visible to families, particularly in newer or rapidly evolving services such as AI chatbots, where the long-term impacts on children are not yet fully understood. Parents' views are therefore important evidence of how families understand and experience risk, but Government should also consider children's reported experiences, independent research, platform risk assessments and expert evidence on emerging harms.

### 2.1.3 Parents favour targeted interventions over a blanket ban

Parents also support targeted interventions over a blanket ban. When asked which alternative options they would support instead of banning social media for under-16s, only 10% selected “None of these – I support a ban on social media for children under 16”. Parents were more likely to support measures such as automatic parental controls for under-16 accounts (39% of parents), child or teen accounts by default (38%), restrictions on certain functionalities (34%), and removing features designed to keep children online for longer (35%) (Figure 5).<sup>32</sup>

**Figure 5. Support among parents for alternative options to a social media ban for under-16s**



This suggests that many parents want stronger action, but favour measures that address specific risks over a blanket ban and which increase parent oversight.

Qualitative research also shows why families are cautious about blunt restrictions. Parents recognise the risk that blunt restrictions may not work as intended.<sup>33</sup>

*“I think it’s [the ban] a great idea in theory and I applaud its intentions, but I don’t see how that’s feasible, because kids will always find a way.” (Dad of boy, 15)*

*“Taking away things just creates a black market and a vacuum for something else much, much darker, much harder to regulate” (Mum of girl, 11)*

Parents and children also recognise the benefits that could be lost through overly broad restrictions:

*“What about all the good things we’ve talked about, learning and creativity, that would be taken away?” (Mum of girl, 11)*

*“[Social media is] how we talk outside of school. So I think if that gets banned, this is not really good.” (Boy, 13)*

#### 2.1.4 A blanket ban could have uneven and unintended impacts

A blanket restriction focused only on social media could also have uneven impacts across children’s online lives. Internet Matters’ research shows that boys spend significantly more time gaming than girls, at 7.5 hours per week compared with 4 hours per week. While social media is used heavily by both boys and girls, we find that girls are more likely to use the most popular social media apps. For example, girls are more likely to use WhatsApp (71% vs 62%), TikTok (57% vs. 49%), Snapchat (47% vs. 38%), and Instagram (46% vs. 39%).<sup>34</sup> If restrictions focus only on popular social media services, but not gaming or other online environments with similar interactive features, they may affect girls and boys differently and overlook risks in other environments, including chat functions, contact from strangers, in-game spending and exposure to age-inappropriate content.

Blanket age restrictions may also have a disproportionate impact on children who place particular value on online spaces. As discussed in Chapter 1, children with additional needs feel more of the benefits of the online world than their peers. Internet Matters’ *DWI Year 4* finds that children with additional needs are more likely than their peers to say the internet is important for finding groups that offer friendship and support (59% for children with additional needs compared to 47% of their peers), and that being online helps them feel comfortable being themselves (52% compared to 42%). Parents reinforce this, with 49% saying that being online has helped their child feel more comfortable with themselves, compared to just 36% of parents of children without additional needs.<sup>35</sup> Given this, it is unsurprising that we often hear from children with

additional needs and their families that they place greater importance on online spaces. For some of these children, online environments can create a space where they can just be themselves, without their disability. Locking them out of these environments could therefore have a stronger negative impact than it would for their peers.

*“I feel completely accepted online.” (Young person with additional needs, aged 15-17)<sup>36</sup>*

There may also be implications for young people’s access to reliable information and civic participation. Internet Matters’ joint research with Full Fact found that 78% of young people aged 13–17 have seen content about news, politics or current affairs online, rising to 81% among 15–17-year-olds. This does not mean that teenagers should have unrestricted access to all social media services or features. However, it does mean that restrictions should be designed carefully, so that they preserve age-appropriate access to reliable information and civic participation opportunities, while addressing the platform features and content risks that make these environments unsafe. This is especially important as the UK looks to lower the voting age to 16.<sup>37</sup>

A further risk is displacement. Some parents warn that a blanket ban or higher minimum age could push children towards harder-to-regulate spaces, rather than reducing risk overall. Parents described the possibility of a “black or grey economy” emerging, or of children moving into “something else much, much darker, much harder to regulate”.<sup>38</sup> This reinforces the need to ensure that any age-based restriction reduces overall harm, rather than simply displacing children into less visible or less safe online environments.

### 2.1.5 Government should take a targeted, risk-based approach

Government should therefore avoid assuming that a blanket social media ban would, by itself, make children safer online. Internet Matters does not support a blanket legal ban on children’s access to social media. A better approach is to identify the services, features and design choices that create the greatest risks for children, and require online services to reduce those risks while preserving children’s access to beneficial, age-appropriate online experiences. This approach would better account for the different ways children use online services, the uneven impacts restrictions may have across groups of children, and the risk that blunt restrictions simply displace children into other, less protected, online spaces.

### 2.2 Age-based protections will only work if minimum ages are effectively enforced

A targeted approach may still require age-based protections, particularly to prevent children’s access to certain features or entire services that cannot provide safe, age-appropriate experiences for younger children. However, age thresholds

will only protect children if they are meaningfully enforced. At present, many children are already using online services below the minimum ages set in those services' terms of service. This suggests that current approaches to enforcing minimum age limits are not enough.

*Internet Matters Pulse* finds that many younger children are using services that set a minimum age of 13. For example, 47% of UK children aged 9-12 use WhatsApp, 32% use TikTok and 22% use Snapchat, despite these services stating that users must be at least 13.<sup>39</sup>

Weak enforcement of minimum age requirements is also evident in children's use of AI chatbots. *Internet Matters' Me, Myself and AI* finds that nearly two-thirds (64%) of children aged 9-17 say they have used an AI chatbot, including 58% of children aged 9-12, despite many popular services setting a minimum age of 13 in their terms of service. *Internet Matters' user-testing* also finds that popular AI chatbots do not have robust age verification mechanisms in place, with services relying largely on self-declaration at sign-up, while others do not require log in for use.<sup>40</sup>

Minimum age rules are also undermined when children can access restricted features despite service policies. For example, children describe being able to or ways of accessing livestreaming on services even where age restrictions are intended to apply:

*"If [going live] needed an ID, I'd use my parent's ID and then if they wanted to upload a photo, I'd go online and upload any." (Boy, 13)<sup>41</sup>*

*"Every time I go live on TikTok, it tells me I have to be 18, but when the AI detects that I'm not 18 they ban me. But they only ban me for 10 minutes and then I can go live again." (Girl, 12)<sup>42</sup>*

This matters because any future age-based requirements will only be effective if online services are required to enforce them effectively. This applies both to minimum ages for whole services and to age restrictions on specific features or functionalities. Government should therefore ensure that services can evidence that their age thresholds are appropriate and that children are not able to easily bypass them. This will require more robust age assurance and appropriate parental involvement, which we discuss in Chapter 3.

### **2.3 Services should have to prove they are safe and age-appropriate for children**

The evidence above points to the need for Government to create a clear framework for when minimum ages are needed, how they should be set, and how they should be enforced. Minimum age requirements should be evidence-based, risk-based and effectively enforced. Online services should be required to demonstrate that their design, defaults, functionalities and safeguards are suitable for the children they are letting onto their services.

The framework should take into account the nature of the service, the age of children using it, the risks created by its features and design, and the effectiveness of the safeguards in place. Relevant factors should include whether children can access features or functionalities that are risky to them ('high-risk features or functionalities'), whether content or users are recommended to them, whether persuasive design features are used, and whether child or teen accounts, safer defaults, reporting tools and parental controls are effective. This would create stronger accountability than the current system and incentivise services to improve the safety of their design and defaults.

If a service wants to be accessible to younger children, it should have to show that the experience it provides is appropriate for that age group. Where a service cannot demonstrate that children of a particular age can use it safely, it should not be able to make that service available to them.

Services should be expected to follow the Government's framework, or provide robust evidence where they believe a different age threshold is justified. They should also be required to show that any age thresholds they set are effectively enforced. Without this, minimum ages risk remaining a matter of platform policy rather than meaningful protection for children.

#### **2.4 Children need age-appropriate access to high-risk features**

Feature-based restrictions are likely to be more proportionate than whole-service bans because they target the parts of online services most likely to expose children to harm, while preserving access to beneficial online experiences. This approach is especially important where the same feature can create similar risks across different environments, including social media, messaging services, gaming platforms, livestreaming services and AI services.

The Government's consultation rightly identifies several functionalities that can create heightened risks for children. Internet Matters agrees that these should be treated as high risk, but different functionalities require different responses. Some should not be available to children at all. Others may be appropriate only for older teenagers, or only where strong safeguards are in place.

The list of functionalities government is considering should also not be treated as closed. New features can emerge quickly, and existing features can change in ways that increase or reduce risk. Government and Ofcom should therefore have clear criteria for identifying additional high-risk features over time. This should include considering the risks created by the feature, how it operates within a service, the age of likely child users, and whether effective safeguards are in place.

There is strong parental support for restricting functionalities government is consulting on. *Internet Matters Pulse* finds that four in five parents (80%) agree that restricting children from accessing certain functions, such as livestreaming or in-app spending, would make the online world safer for children.<sup>43</sup>

Internet Matters’ position on the functionalities identified in the consultation, is set out below. We recommend that Government also consider restrictions on in-app spending, gifting, rewards and loot box-style mechanics, given the financial, behavioural and safeguarding risks these features can create for children.

<b>Functionality</b>	<b>Internet Matters’ position</b>
<b>Sending or receiving nude images/videos</b>	Should not be available to under-18s.
<b>Disappearing content</b>	Should not be available to under-16s. 16–17-year-olds should have opt-outs, reporting routes and evidence-preservation safeguards. Where these safeguards are not in place, further age restrictions should apply.
<b>Hosting livestreams</b>	Should not be available to under-16s. 16–17-year-olds should only be able to host livestreams where strong safeguards are in place, including limits on gifting, comments, reactions, screen recording and contact from unknown adults. Where these safeguards are not in place, further age restrictions should apply.
<b>Contact with strangers</b>	Private or direct contact from unknown adults should be restricted for under-16s. Moderated, age-appropriate public interaction should be treated differently. 16–17-year-olds should have strong account safeguards, including defaults that limit contact from unknown adults.
<b>Location sharing</b>	Risky location visibility should be restricted for under-16s, especially where precise or live location is visible to other users. Location sharing with a parent or carer for safety purposes should be treated separately.
<b>In-app spending, gifting, rewards and loot box-style mechanics*</b>	Children’s access should be limited where features are more likely to cause harm, including loot box-style mechanics, repeat purchases, in-game currencies, time-limited offers, gifting or user-to-user financial interactions.

\* Additional functionality for Government to consider restricting.

### 2.4.1 Children under 18 should not be able to send or receive nude images or videos

**Children under 18 should not have the ability to send or receive nude images or videos.** This functionality creates clear risks, including the creation and circulation of child sexual abuse material, sexual coercion, image-based abuse, child-on-child sexual harassment and sextortion.<sup>44</sup> Where a child shares an intimate image of themselves, they may quickly lose control over where it goes, who sees it, whether it is saved or reshared, and whether it is used to pressure, threaten or exploit them. While the specific functionality under consideration is

the ability to send nude images or videos, effective prevention will require safeguards across the services, devices and operating systems through which children share, receive, save or reshare this content.

Evidence from the Internet Watch Foundation (IWF) shows why these risks need to be taken seriously. The IWF finds that 27% of the child sexual abuse images and videos it identified in 2025 were recorded as “self-generated”, while cautioning that this term should not imply children are responsible for their own abuse.<sup>45</sup> Children may be groomed, deceived, coerced or extorted into producing or sharing images. The NSPCC also defines online sexual extortion as a form of blackmail involving threats to share nude or semi-nude images or videos to extort money or force someone to do something against their will.<sup>46</sup> This means services should not treat children’s nude image-sharing as a matter of individual choice or user behaviour alone. The functionality can facilitate the creation and circulation of child sexual abuse material, including in circumstances where children have been pressured, manipulated or exploited.

AI tools are adding to these risks by making it easier to create, manipulate and recirculate sexualised images of children, including imagery based on real children or known victims. IWF has warned that AI is contributing to record levels of online child sexual abuse, including a major increase in AI-generated child sexual abuse videos in 2025.<sup>47</sup> UNICEF has also described AI-powered image and video generation tools that produce child sexual abuse material as a significant escalation in risks to children.<sup>48</sup>

Internet Matters’ own research also shows that the abuse of images is an issue for children. Almost half (49%) of teenagers aged 13-16 have heard about image-based sexual harassment or abuse happening to another young person they know, including images being shared without consent, threats to share images, and the creation of sexual images without consent, including deepfake nude images.<sup>49</sup>

Our research finds that children with additional needs are disproportionately affected. 11% have had a sexual image shared without their consent, compared with 4% of their peers without additional needs. They are also more likely to have felt pressure to share a nude image online, with nearly a quarter (23%) of children with additional needs reporting this compared to 12% of their peers.<sup>50</sup>

Children and parents support stronger platform action to prevent young people sharing or receiving nude images. Internet Matters’ research finds that that 81% of 13-16-year-olds believe sharing nude images is always harmful to the young people involved, and 84% agree social media platforms should do more to prevent young people from sharing nudes. Parents share these concerns: 87% say platforms should do more to prevent young people sharing and receiving nude images, and 70% say young people sending and receiving nude images was a major concern for them as a parent.<sup>51</sup>

Parents also view this as the highest-risk functionality. When asked about a range of functionalities, 56% of parents said no child should be able to send or receive nude images or videos.<sup>52</sup>

Government should put in place safeguards that prevent children being placed in these situations in the first place, rather than relying only on reporting or removal after an image has been shared. Given that children must be 18 to access pornography, it is reasonable that the ability to send or receive nude images or videos should also be subject to a minimum age of 18. While the age restriction should focus on the ability to send or receive nude images or videos, Government should also consider the wider ecosystem that enables this content to be shared, received, saved or reshared, including device-level and operating-system-level controls where relevant. This should sit alongside strong safeguards, accessible reporting routes, education on sexual image sharing, and measures to detect, prevent and disrupt the creation and circulation of sexual images of children.

Government should also ensure that its upcoming ban on nudification apps and services captures all services that enable sexualised or intimate images to be created without consent, even where they present themselves as general-purpose image-editing tools. Internet Matters' research finds that nudification tools are widely available, cheap and easy to use, with 21 distinct nudification sites appearing on the first page of search results across three major search engines. None of the 21 sites reviewed required users to verify their age before viewing the site, and while some stated that consent was required, the research did not identify mechanisms in the upload process to verify or enforce consent.<sup>53</sup> The ban should therefore apply to services whose purpose or functionality is to create nude or deepfake sexual images, regardless of how they describe or market themselves.

#### 2.4.2 Disappearing content should be restricted

##### **Children under 16 should not have access to disappearing content features.**

Access for children aged 16-17 should depend on the relevant safeguards being in place. This is particularly important where disappearing content is used as part of private messaging or image and video sharing. The risk is particularly acute in these contexts because harm may occur away from public scrutiny and involve content that a child needs to evidence quickly, such as nude images, threats, bullying or coercive messages.

Disappearing content is not inherently harmful. However, where harmful messages, threats or images disappear quickly, children may be less able to show a trusted adult what has happened,<sup>54</sup> parents may have less information to support them, and harmful contact or content may be harder to report, investigate or act on.<sup>55</sup>

Internet Matters' research suggests that disappearing content can play a role in harmful experiences online. Among teenagers aged 13-16 who had received an

unwanted nude image, 58% had received it on Snapchat, a service built around temporary messaging and disappearing content features. This rises to 73% among girls, compared with 39% of boys.<sup>56</sup>

Disappearing content is also relevant beyond sexual image-sharing. *Internet Matters Pulse* finds that, among children who had experienced online bullying, trolling or abuse from people they do not know, the most commonly cited platform was Snapchat, selected by 34% of children who had experienced this harm.<sup>57</sup> This does not mean that harms only occur on Snapchat, or that all disappearing content is harmful. However, it shows why services built around temporary private messaging or image-sharing need particularly strong safeguards.

Government should therefore consider both age-appropriate restrictions on high-risk uses of disappearing content and the safeguards services have in place. Children under 16 should not have access to these features. For 16–17-year-olds, services should provide clear opt-outs, simple reporting routes, evidence preservation following a report, clear information about what disappearing content does and what action the platform will take when harm is reported, and a route to challenge where no action is taken. Where services cannot do this for 16-17 year olds then they should not have access to this feature.

### 2.4.3 Children under 16 should not be able to host livestreams

**Children under 16 should not be able to host livestreams.** 16-17-year olds who are permitted to host livestreams should have strong safeguards, including restrictions on comments, gifting, reactions, screen-recording and contact from unknown users. Children's ability to watch livestreams may require different safeguards depending on the content, audience, interaction features and commercial prompts available.

Livestreaming is already a common part of children's online lives. *Internet Matters Pulse* finds that 62% of children have either watched livestreamed content or livestreamed their own content. 58% have watched content streamed live, while 13% have livestreamed their own content. This includes 13% of children aged 9-15 who are livestreaming their own content. Twitch is the largest livestreaming platform in our data, used by 7% of children, with boys more likely than girls to use it (10% of boys c.f. 3% of girls).<sup>58</sup>

Hosting livestreams carries particular risks because livestreams unfold in real time.<sup>59</sup> This can limit opportunities for moderation or intervention before a child experiences harm. Interactive features such as comments, reactions and gifting can also create pressure on children to respond to viewers in the moment, including unknown users or adults. As a result, livestreaming can intensify risks that children already face online, including exposure to harmful content, bullying, unwanted contact and pressure from other users.

Children who livestream report higher levels of harm across several areas. For example, 17% of children who livestream their own content report online bullying from people they know, compared with 11% of all children; 16% report being asked for or giving away personal information online, compared with 10% overall; and 35% report coming across content promoting dangerous stunts or challenges, compared with 22% overall.<sup>60</sup> This does not prove that livestreaming causes these harms, but it does suggest that children who livestream are a higher-risk group.

Livestreaming can also create serious safeguarding risks, including grooming and child sexual exploitation. Government guidance on online child sexual exploitation and abuse identifies livestreamed abuse as one way offenders use technology to harm children.<sup>61</sup> The Independent Inquiry into Child Sexual Abuse also identifies livestreaming as presenting particular challenges because abuse can occur in real time, across borders and in ways that are difficult for law enforcement and platforms to detect and disrupt.<sup>62</sup>

Parents support stronger restrictions. *Internet Matters Pulse* finds that 21% of parents do not support children having access to livestreaming themselves or watching others' livestreams, and 45% support a minimum age of 16 or above.<sup>63</sup>

Given the potential level of harm and support from parents, government should consider stronger restrictions on children's ability to host livestreams. Children under 16 should not be able to host livestreams, while 16–17-year-olds should only be able to do so with age-appropriate safeguards. This should include restrictions on unknown adults viewing, and restriction on commenting, gifting, recording or contacting the child. Children's ability to watch livestreams may require different safeguards depending on the content, audience, interaction features and commercial prompts available.

Some services such as TikTok and YouTube already apply age-based restrictions to livestreaming, illustrating that age-based restrictions on livestreaming are already recognised by some services as necessary protections.<sup>viii</sup>

#### 2.4.4 Stranger contact from unknown adults should be restricted for children

**Children under 16 should not be contactable privately or directly by unknown adults.** This should include features that allow adults to message, follow, recommend, invite or otherwise initiate contact with child users, including through direct messages, friend or follow prompts, group chat invitations, network recommendations, livestreaming or gaming features.

Stranger contact is high risk because it can enable adults to identify, approach and build relationships with children away from trusted adults or public scrutiny. Ofcom's Illegal Harms Register of Risks notes that online grooming involves

---

<sup>viii</sup> For more information, see TikTok's [LIVE Safety Guide](#) and YouTube's guide on [how to avoid restrictions on YouTube live streaming](#).

identifying and contacting a child, and that functionalities such as direct messaging can allow abusers to identify and contact children.<sup>64</sup> According to Ofcom, direct messaging can allow perpetrators to build relationships away from public view and parental supervision, while user connection features can enable perpetrators to establish contact with child users and begin communication.

*Internet Matters Pulse* finds that 25% of children say a stranger has contacted them online.<sup>65</sup> Parents support stronger restrictions on this feature: 35% say features that enable contact with strangers should be restricted for all children, while a further 35% support a minimum age of 16 or above.<sup>66</sup> Children also describe stranger contact as a common feature of their online lives:

*“On Instagram, it’s so common I barely even think about it too much. I get loads of strangers messaging me, following me, trying to put me in group chats with other strangers. I usually exit and block, it’s just annoying.” (Girl, 16)<sup>67</sup>*

*“It was some random guy who added people and was trying to get them to send him pictures. I panicked a bit, so I just blocked him.” (Girl, 15)<sup>68</sup>*

However, “stranger contact” needs careful definition. The aim should not be to prevent all interaction with new people online. Some moderated, age-appropriate communities can support learning, identity, friendship and peer support. The higher-risk scenario is where unknown adults can contact children privately or directly, or where services encourage children to expand their networks through friend suggestions, group chat prompts or network recommendations. Restrictions should therefore focus on private or direct contact from unknown adults, while treating moderated, age-appropriate public interaction differently.

Government should therefore consider stronger restrictions on private or direct contact from unknown adults across services used by children. At a minimum, under-16s’ accounts should not be contactable by unknown adults by default; adults should not be recommended to child users, or child users to adults; and children should not be added to private groups, chats or livestream interactions by unknown adults. There could also be a role for parents in approving requests. For 16–17-year-olds, services should provide strong account safeguards, clear controls, reporting routes, effective moderation and age assurance.

#### 2.4.5 Location-sharing restrictions must distinguish between safety tools and risky location visibility

**Risky location visibility should be restricted for under-16s, especially where a child’s precise or live location is visible to other users.** This should be treated separately from location sharing with a parent or carer for safety purposes, which some families use to support children’s safety and independence. Government should therefore distinguish between tools that help parents and carers support children, and forms of location visibility that expose children to other users or enable location-based contact.

Some location tools may be useful for families. For example, they may help parents or carers support children's growing independence, travel or safety. Internet Matters' *Digital Dilemmas* finds that parents recognise practical benefits from children having smartphones, including being able to maintain contact with their child and feeling more confident that their child is safe. This is important context: parents may see location tools as part of how they manage risk, rather than as a risk in themselves.<sup>69</sup>

However, location sharing can create serious risks where a child's precise or live location is automatically displayed, shared by default, or made visible to other users without their explicit permission. This may expose children to grooming, stalking, harassment, coercive behaviour or unwanted contact, particularly where location sharing is combined with public profiles, direct messaging or stranger contact.<sup>70</sup>

Parents recognise the risks of location sharing: 28% do not support children being able to share their location on platforms, and 38% support a minimum age of at least 16.<sup>71</sup>

Government should therefore focus restrictions on risky location visibility and location-based contact, particularly where a child's precise or live location can be seen by other users. This should include location sharing that is on by default, difficult for children to understand or change, or linked to public profiles, direct messaging, friend suggestions or contact from unknown users. Where location-sharing features remain available to older children, they should be off by default, clearly explained, easy to change, and designed so that children and parents understand who can see location information and when.

#### 2.4.6 Government should consider restricting high-risk in-app spending, gifting, rewards and loot box-style mechanics

Government should consider restricting children's access to in-app spending, gifting, rewards and loot box-style mechanics as an additional high-risk functionality. Restrictions should focus particularly on features that involve repeat purchases, in-game currencies, time-limited offers, randomised rewards, gifting or financial interactions between users. These features can create financial harm, encourage impulsive or repeated spending, and in some contexts create risks of grooming or coercion.

Internet Matters' evidence shows that online spending is already an issue for children and families. *The DWI Year 5* finds that one in ten (9%) children have reported spending large sums of money in apps or games, rising from 5% in 2022. This is even higher for children with additional needs (13%). Parents are also concerned: 49% are worried about their child spending money online. Parents of children with additional needs are more likely to report that their child spends money in apps or games without realising compared to parents of children without additional needs (47% c.f. 23%).<sup>72</sup>

These risks are not only about individual purchases. Spending can be shaped by the design of digital services. Features such as in-game currencies, bundled currency packages and time-limited offers can make spending feel less visible, more urgent or more socially expected, lowering the barriers to repeat or impulsive purchases.

Loot box-style mechanics create an additional concern because children may spend money without knowing what reward they will receive. GambleAware's research has highlighted links between loot boxes, gambling-like behaviours and potential financial and psychological harms,<sup>73</sup> while the House of Commons Library notes that risks associated with loot boxes are likely to be higher for children and young people.<sup>74</sup>

Gifting creates further risks where children can give or receive gifts, rewards, virtual items or currency from other users. In some contexts, gifts can be used to reward behaviour, build relationships, create a sense of obligation or encourage children to keep engaging with unknown users. Ofcom's additional safety measures consultation notes evidence that groomers may offer in-game or in-app gifts or currency to coerce children, and proposed removing gifting from children's livestreams to reduce the ability of viewers to entice or encourage children into sexual behaviour or other harm in return for a reward.<sup>75</sup>

Parents support age restrictions on in-app or in-game purchasing. *Internet Matters Pulse* finds that 17% believe no child should have access to this feature, while 45% believe access should be restricted to those aged 17 or above.<sup>76</sup>

Government should therefore limit children's access to the highest-risk forms of in-app spending, gifting, rewards and loot box-style mechanics. These restrictions should apply wherever children can access these features, including games, livestreaming platforms, social media services, app stores and other online environments. At a minimum, children should not be exposed to spending mechanics that rely on randomised rewards, pressure to purchase quickly, repeated spending loops, or gifts and virtual currency from unknown users.

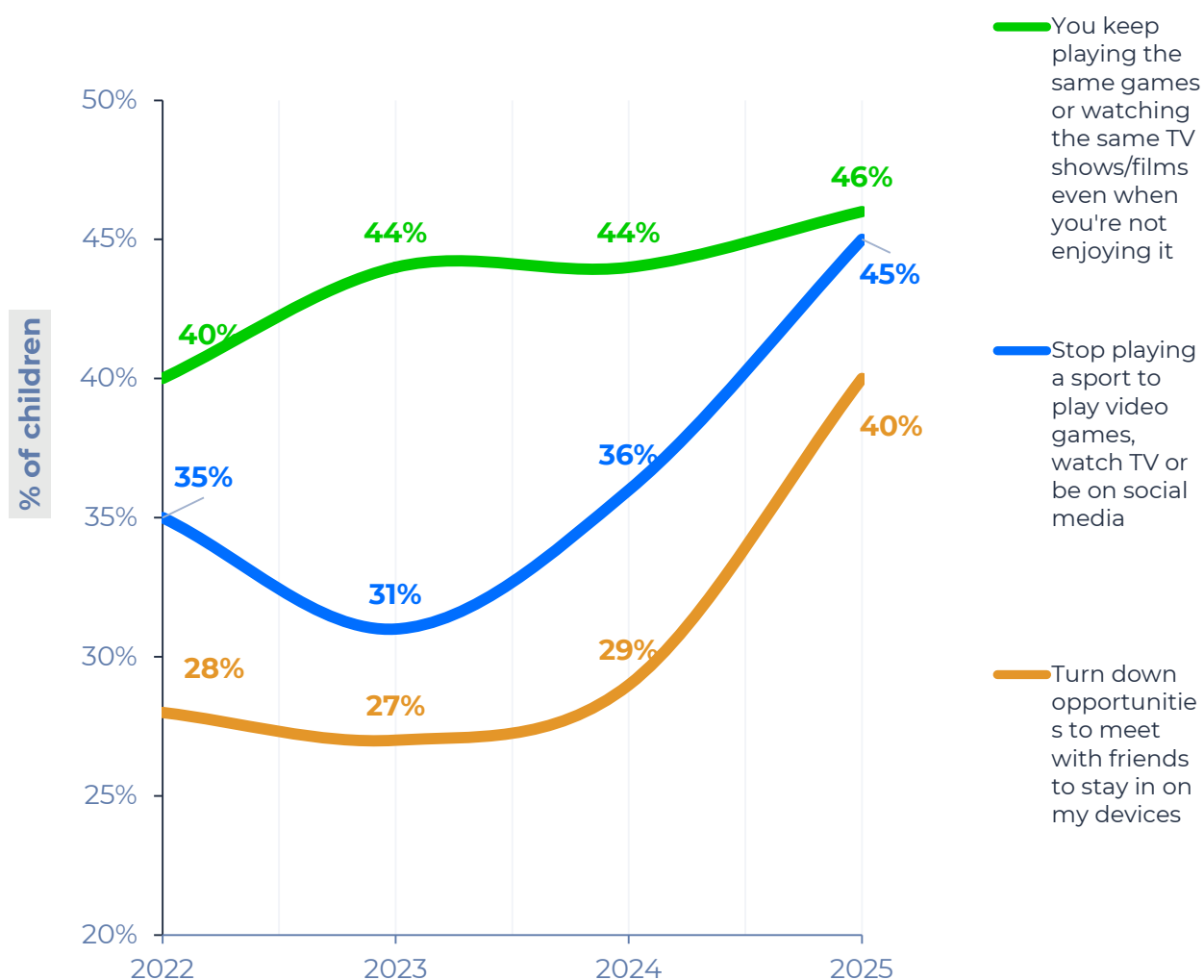
## **2.5 Online services should address features that make it harder for children to regulate time online**

Alongside restricting access to specific functionalities, government should address the design features that make it harder for children to regulate the amount of time they spend online. The issue is not simply that children are online, but that many children report struggling to disengage, with consequences for sleep, physical activity, social life and wellbeing. Screen time guidance and controls can help families set boundaries, but they should sit alongside action on persuasive design features that encourage prolonged or compulsive use.

The amount of time children spend online is one of the most significant concerns for families. 76% of parents are concerned about children spending too much

time online, 44% of children report doing so.<sup>77</sup> Furthermore, Internet Matters' *DWI Year 5* shows that a growing number of children are struggling to regulate the amount of time they spend online, with consequences for their wellbeing (Figure 6). For example, nearly half of children (46%) keep playing the same games or watching the same shows or films even when they are not enjoying them (c.f. 40% in 2022); 45% have stopped playing sport or doing exercise because they want to play video games, watch TV or be on social media (c.f. 35% in 2022); and 40% say they turn down opportunities to meet with friends to stay in on their devices (c.f. 28% in 2022).<sup>78</sup>

**Figure 6. Children are increasingly finding it difficult to disconnect**



**Figure 6. Children are increasingly finding it difficult to disconnect** | Data from *Children's Wellbeing in a Digital World Year 5 (2026)*.  
 Base: All children 2022 (1138); 2023 (1001); 2024 (1054); 2025 (1270). Q: How often do these things happen? / Q: How much do each of these things sound like you? / Q54. How often do you do any of the following things?

These patterns are taking a physical, emotional and social toll. The *DWI Year 5* finds that 29% of children report that spending a lot of time online negatively affects their physical health, up from 18% in 2022. More children also say that missing out on friends' social media activity makes them upset (39%, c.f. 24% in 2022). Parents are seeing this too: 37% now report that their child turns down opportunities to meet friends so they can stay in on their phone, computer or games console, compared to 26% in 2022.<sup>79</sup>

Time online also correlates with higher rates of harm. *The DWI Year 5* groups children into quartiles based on the average amount of time they spend online across a range of activities. Among children in the highest quartile of time spent online, 80% report experiencing online harm, compared to 52% of children in the lowest quartile. Children in the highest-use group are also more likely to encounter specific risks, including violent content, contact from strangers, and abusive or upsetting messages from strangers or people they know.<sup>80</sup>

However, this does not mean the policy response should focus only on the total number of hours children spend online. Findings from Internet Matters' *Connected and Conflicted* similarly show that experiences of online harm increase as time spent on social media rises. They also show that children who use social media more actively - such as posting or commenting frequently - are more likely to experience harm than more passive users who mainly browse or scroll.<sup>81</sup> This suggests that children's risk is shaped not only by time spent online, but by the activities they engage in, the features they use, and the way services are designed.

Persuasive design features are central to this picture. Features such as infinite scroll, autoplay, recommender systems, notifications, streaks, likes and comments can make it harder for children to stop using a service, even when they want to. They can also shape what children see and how often they are encouraged to return. Internet Matters' research finds that children and parents recognise these dynamics, describing how algorithms, notifications and social pressure can keep children online for longer or expose them to unsuitable content.<sup>82</sup>

*"My screentime is like 8 hours a day and in that time I'm not doing anything else. I'm just eating, then going on my phone, then going on my iPad. I'm just on my phone and I'm forgetting about homework." (Girl, 12)<sup>83</sup>*

*"I definitely say I spend a lot of time on my phone. I'm on it at 3AM on a school night." (Girl, 16)<sup>84</sup>*

*"When I'm going to sleep, I'll open TikTok and I'll be on it for an hour. It does disrupt [my sleep] quite a bit." (Boy, 15)<sup>85</sup>*

*"The short videos are so easily accessible to scroll. In each video you see a new thing. And it's the burst of dopamine. You want to continue scrolling." (Boy, 15)<sup>86</sup>*

*"[Social media apps are] designed to increase the amount of time you spend watching, not the amount of fulfilment you get from it, which can lead to that dissatisfied feeling after." (Boy, 15)<sup>87</sup>*

*"If you encourage the algorithm to show you it, you can see a lot of car crashes, shootings. I find they kind of promote that stuff when you first download the app. You can get away from it if you start interacting with other videos, but it pushes it at the start." (Boy, 17)<sup>88</sup>*

Parents support practical measures to help children manage time online. *Internet Matters Pulse* finds that 90% of parents support either daily screen time limits (14%), restricting overnight access for individual apps (15%) or both (61%).<sup>89</sup> These measures should not rely solely on parents finding and setting controls themselves. Where services know or have reason to believe a user is a child, they should provide age-appropriate defaults and tools that help children disengage, such as app-level limits, overnight restrictions, notification controls and prompts to take breaks.

Government should therefore address persuasive design as part of the wider child safety framework. This should include requiring services to assess how design features affect children's ability to disengage, and to introduce age-appropriate defaults that reduce compulsive use, harmful displacement and exposure to risk. This could include limits on autoplay, prompts to take breaks, restrictions on overnight notifications, greater control over recommender systems, and settings that make it easier for children and parents to manage time online.

At the same time, Government should recognise that online time can bring benefits. This is particularly important for children with additional needs or vulnerabilities, as discussed in Chapter 1. Some children rely on online spaces for social connection, emotional regulation, accessibility, support or community. The right approach is not to treat all time online as harmful, but to reduce compulsive use and harmful displacement while preserving children's access to the benefits of online life.

## **2.6 AI chatbots need urgent, child-centred regulation**

AI chatbots can offer children meaningful benefits when they are designed and used appropriately. However, they also introduce new and amplified risks because they are interactive, personalised and conversational. The long-term impacts of children's use of AI chatbots are not yet fully understood, particularly where tools are emotionally responsive, companion-style or highly personalised. Government should urgently bring all AI chatbots into scope of the Online Safety Act's children's safety duties and ensure providers are required to design age-appropriate experiences from the outset.

Children are already using AI chatbots for different reasons. Among children who use AI chatbots, the most common reasons are help with schoolwork or homework (42%), finding information or learning about something (40%), and curiosity (40%). There are many positive use cases with nearly half (47%) of children aged 15-17 who use AI chatbots using them to support schoolwork, including revision, writing support, language learning and building understanding of new concepts.<sup>90</sup> Some children also use AI chatbots to ask questions when they feel embarrassed, uncertain or reluctant to ask an adult.

These potential benefits are real, but they depend heavily on design. AI chatbots used by children should be age-appropriate, accurate and transparent, with clear limits on mature content, sensitive advice, emotional dependency and personalised interactions. They should not be treated as substitutes for trusted adults, teachers, mental health support or safeguarding routes.

Children are also using AI chatbots in emotionally driven ways. Almost a quarter (23%) of children who use AI chatbots have used them to seek advice, and over a third (35%) say chatting with an AI chatbot feels like talking to a friend, with the latter figure rising to 50% for children with additional needs. One in eight (12%) children who use AI chatbots say they use them because they have no one else to speak to.<sup>91</sup>

These findings are concerning because children may place high levels of trust in AI-generated responses. Internet Matters' research finds that 58% of children who use AI chatbots think using an AI chatbot is better than searching for something themselves, while 40% have no concerns about following advice from an AI chatbot. Among children with additional needs who use AI chatbots, 50% have no concerns about following chatbot advice.<sup>92</sup>

These risks underline the need for a child-centred regulatory approach to AI chatbots. The aim should not be to restrict all children's access to all AI-enabled tools, but to ensure that services accessed by children are designed around their age, needs and vulnerabilities, and that the highest-risk AI chatbot experiences are subject to stronger safeguards.

Government should require AI chatbot providers to set, evidence and enforce appropriate minimum ages based on risk. Parents also support clearer age boundaries for AI chatbot use. *Internet Matters Pulse* finds that 74% of parents support a minimum age of 13 or above for AI chatbots, including 27% who support a minimum age of 16 or 17, and 10% who say no child should be able to access them.<sup>93</sup> This suggests that while families may recognise the benefits of AI chatbots, they also expect clearer age-appropriate limits and safeguards.

Higher minimum ages are likely to be appropriate for AI chatbots designed for companionship, romantic or emotionally responsive interaction, or where users can create, customise and share chatbots with others. However, not every AI-enabled tool should be treated in the same way. A limited AI search function,

educational support tool or information service with clear limits on the content and advice it can provide may not require the same minimum age as a companion-style chatbot.

Minimum age requirements should be accompanied by restrictions on functionalities or features that pose heightened risks to children's safety and wellbeing. This should include features that enable emotionally responsive or companion-style interactions, romantic or sexual roleplay, mature or age-inappropriate content, image, audio or video generation, long-term memory across sessions, personalised advice on sensitive topics, and the ability for users to create, customise or share chatbots with others. Features that mimic empathy, friendship or romantic connection require particular scrutiny because they may increase children's trust in AI-generated responses, blur relationship boundaries and encourage over-reliance.

Alongside age-restricting certain functionalities or features, AI chatbot providers should also build safety and media literacy into the user experience. This could include clear reminders that children are interacting with an AI system, limits on continuous or emotionally intense conversations, prompts that encourage children to speak to a trusted adult, signposting to trusted support, and age-appropriate explanations of how the AI chatbot works and why its responses may be inaccurate or incomplete. These measures could help children use AI chatbots more safely while preserving beneficial uses for learning, creativity and information-seeking.

AI chatbot regulation should also include effective age assurance, age-appropriate content filtering, parental controls, transparency about how conversations are stored or used, and restrictions on mature, sexualised or emotionally manipulative interactions. The aim should be to preserve beneficial uses of AI while preventing children from being exposed to chatbot experiences that are inappropriate for their age and stage of development.

Alongside these safeguards, Government should clarify how AI chatbots accessed by children are regulated and close gaps in the current framework. Not all AI chatbots are clearly covered by the Online Safety Act. Where a chatbot does not involve user-to-user content or search functionality, it may fall outside parts of the current framework. The Crime and Policing Act provides a mechanism for the Secretary of State to make regulations relating to illegal content on AI chatbots, but not content that is legal but harmful to children, or features and functionalities that may be harmful to children. Government should urgently ensure that these regulatory gaps are addressed, particularly for AI chatbots used by children.

## **2.7 What Government must do**

A safer online world for children will not be achieved through blanket bans alone. Government should focus on the services, features and design choices most likely

to expose children to harm, while preserving children's access to beneficial, age-appropriate online experiences.

Many of these interventions will depend on services being able to identify child users and apply protections according to their age. As set out in Chapter 3, this means age assurance must be effective, proportionate, privacy-preserving and accessible, and should be used not only to restrict access, but to deliver safer, age-appropriate experiences. Government should therefore focus on:

- **Developing a risk-based framework for minimum ages.** Government should set clear criteria for when minimum age requirements are appropriate, based on the service's risk profile, likely child users, features, design and safeguards. Services should be expected to follow this framework, or provide robust evidence for why they believe a different age threshold is justified. They should also be required to show that age thresholds are effectively enforced, supported by proportionate and privacy-preserving age assurance.
- **Restricting children's access to the highest-risk functionalities.** Government should prioritise restrictions where specific features create heightened risks. Children under 18 should not be able to send or receive nude images or videos. Children under 16 should not be able to host livestreams, and should face restrictions on disappearing content where it makes harm harder to evidence. Government should also consider age-appropriate restrictions on private contact from unknown adults, risky location visibility, in-app spending, gifting and rewards. These restrictions should apply across all services used by children, not only those labelled as social media.
- **Addressing persuasive design through platform design.** Government should tackle features that encourage prolonged or compulsive use, such as infinite scroll, autoplay, recommender systems, notifications, streaks and affirmation metrics. Screen time guidance, time limits and parental controls may help families set boundaries, but they should sit alongside requirements on services to reduce design features that encourage prolonged or compulsive use.
- **Urgently regulating AI chatbots accessed by children.** Government should clarify how AI chatbots accessed by children are regulated and require providers to design age-appropriate experiences. Stronger expectations are needed for AI chatbots that provide companion-style, emotionally responsive, romantic, mature or highly personalised interactions.
- **Ensuring protections work for different children.** Government should ensure age restrictions, feature restrictions and design requirements

reflect the different ways children experience the online world. This includes children with additional needs or vulnerabilities, who may face higher risks online while also deriving important benefits from online spaces. Measures should be proportionate, privacy-preserving and clearly explained to children and parents.

This approach would better reflect how children use digital services in practice: not as a simple choice between access and exclusion, but as a question of whether services are safe, age-appropriate and accountable for the experiences they provide.

## Chapter 3: Effective compliance and enforcement of online safety rules

Minimum ages and feature restrictions will only protect children if they are effectively enforced. Internet Matters' evidence shows that children are accessing services below stated minimum ages, and that age checks can be easy to bypass. Government should therefore focus on whether age assurance works in practice, not simply whether services have introduced an age check.

Age assurance should also be used to support safer, age-appropriate experiences for children, not only to block access to services. It should help services apply appropriate defaults, content restrictions and feature limits. However, age assurance must be privacy-preserving, proportionate, accessible and trusted by children and parents.

This chapter argues that Government and Ofcom should set clear expectations for effective age assurance, including how services should address common workarounds, protect privacy, support parental involvement where appropriate, and report on whether age checks are working in practice. It also argues that Government should avoid over-reliance on VPN restrictions and focus instead on the requirements placed on platforms.

### 3.1 Age restrictions must work in real-world conditions

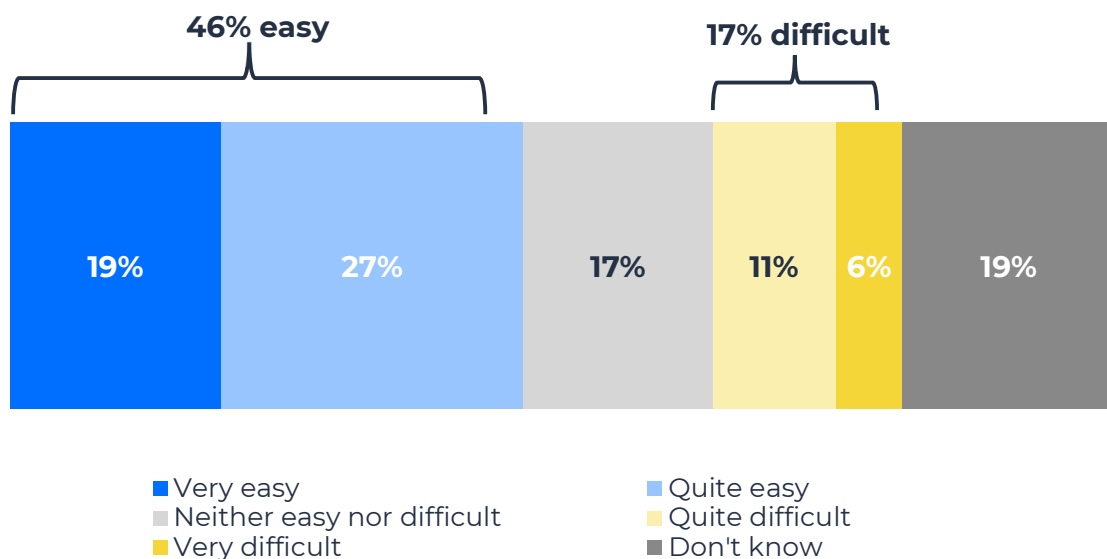
Age restrictions will only be meaningful if services can show that age assurance is effective in practice. This means age checks must be robust enough to identify children accurately, apply protections to both new and existing accounts, and address predictable workarounds.

As set out in Chapter 2, children are already using services and features below stated minimum ages. One reason for this is that some age checks remain too easy for children to get around. Internet Matters' research finds that 46% of children believe age checks are easy to bypass (Figure 7), and 32% say they have bypassed age checks in a two month period.<sup>ix</sup> Children report using a range of methods, including entering a fake birthdate, using someone else's login or device, using someone else's ID, submitting random photos or videos, altering their appearance, or retrying checks after a failed attempt.<sup>94</sup>

---

<sup>ix</sup> As the survey was conducted September – October 2025, the two-month period we asked children about refers to approximately mid-July – end-September 2025.

**Figure 7. Children’s perception on how easy age checks are to bypass**



**Figure 7. Children’s perception on how easy age checks are to bypass** | Data from [The Online Safety Act: Are children safer online?](#) (2026)  
 Base: All children (1270). Q: How easy or difficult do you think it is to get past age verification?

Children and parents describe these workarounds themselves:

*“I did catch my son using an eyebrow pencil to draw a moustache on his face, and it verified him as 15 years old.” (Mum of boy, 12)<sup>95</sup>*

*“I’ve seen clips of people online where they’ll get clips of video game characters like turning their head and use it for age verification.” (Girl, 11)<sup>96</sup>*

These examples show why the effectiveness of age assurance should be judged by how it works in real-world conditions, not only by whether a service has introduced an age check. Services should be required to demonstrate that their age assurance can address forms of circumvention, including the workarounds children already report using. This is particularly important given that many children are already using services below stated minimum ages.

### **3.2 VPN restrictions should not be the primary response to circumvention**

Government should not treat VPN restrictions as the primary response to children bypassing online safety rules. Internet Matters’ evidence suggests that children are more likely to get around age checks through fake ages, shared accounts, shared devices or weak verification processes than by using VPNs.

Internet Matters’ research finds that only 7% of children had used a VPN to get around age checks, while more common methods included entering a fake

birthdate (13%), using someone else's login (9%), and using someone else's device (8%).<sup>97</sup>

Furthermore, *Internet Matters Pulse* found no statistically significant increase in children's VPN use after online age checks were introduced as part of the Online Safety Act. 8% of children had used a VPN in the past 12 months (c.f. 10%, 12 months prior), with the most common reasons relating to data protection or accessing restricted entertainment content, rather than bypassing online safety rules.<sup>98</sup>

Government should also recognise that VPNs have legitimate uses. They can support privacy, security, data protection, access to work or education systems, and safe browsing on public networks.<sup>99</sup> Requiring age checks to access VPNs could therefore create privacy and trust concerns, particularly if adults and children are asked to verify their age to use a privacy-enhancing tool.

This does not mean VPN use should be ignored. Government should continue to monitor whether children's use of VPNs changes over time, particularly if VPNs become easier for children to access. At present, some VPNs may be less accessible to children because they require payment, a subscription or access to an adult's payment method. However, VPNs are also increasingly bundled into other products or offered for free as part of wider services, which could increase children's access over time. Parents and carers may therefore need support to understand when VPNs are being used and what risks they may create.

Government should therefore keep VPN use under review, but avoid treating VPN restrictions as the main response to circumvention unless there is stronger evidence that VPNs are becoming a significant route for children to bypass online safety protections. The current priority should be strengthening the requirements on platforms to make age assurance effective and addressing the workarounds children are already using.

### **3.3 Age assurance should be used to provide to safer, age-appropriate experiences**

Age assurance should not be used only to block children from services they should not access. It should also help services provide age-appropriate experiences for children as they grow older.

This means services should use age information to apply appropriate settings, safeguards, content restrictions and feature limits. For example, a child user should not only be prevented from accessing age-inappropriate services or features; they should also receive safer defaults, stronger privacy settings, appropriate reporting routes, and limits on certain functionalities where they are allowed to use a service.

### **3.4 Age assurance must protect privacy and work for different users**

Wider use of age assurance could improve children's safety, but only if people trust it and can use it. Government should avoid assuming that one age assurance method will work for every user, service or situation. Services should ensure that age assurance is proportionate to the level of risk and accessible to different users.

Privacy and data use are central to trust. Internet Matters' research finds that parents' and children's top concerns about age assurance relate to privacy and data use: 43% of parents and 31% of children are concerned about privacy, while 35% of parents and 30% of children are concerned about how their data will be used.<sup>100</sup>

Services should minimise data collection, avoid unnecessary retention of sensitive or biometric information, and clearly explain what data is collected, why it is needed, how it will be used, how long it will be kept, and what alternatives are available.

Age assurance also needs to work for people in different circumstances. Some children, parents and adults may not have access to photo ID, smartphones, digital identity tools, mobile contracts, banking access, stable internet, or the confidence to use particular verification methods. Systems should also be tested to ensure they do not work less well for particular groups, including by age, gender, ethnicity, disability or appearance. Users should also have accessible ways to challenge or correct an incorrect age assessment.

Government should therefore require age assurance approaches to be privacy-preserving, accessible and proportionate to the level of risk. Services should be able to explain why a particular method is appropriate, what data it collects, how it protects users' privacy, and how users who cannot complete that method will be supported.

### **3.5 Parents should be involved in account creation, but not made responsible for weak systems**

Parental involvement should support safer online experiences, but it should not replace services' responsibility to enforce age rules and design age-appropriate experiences.

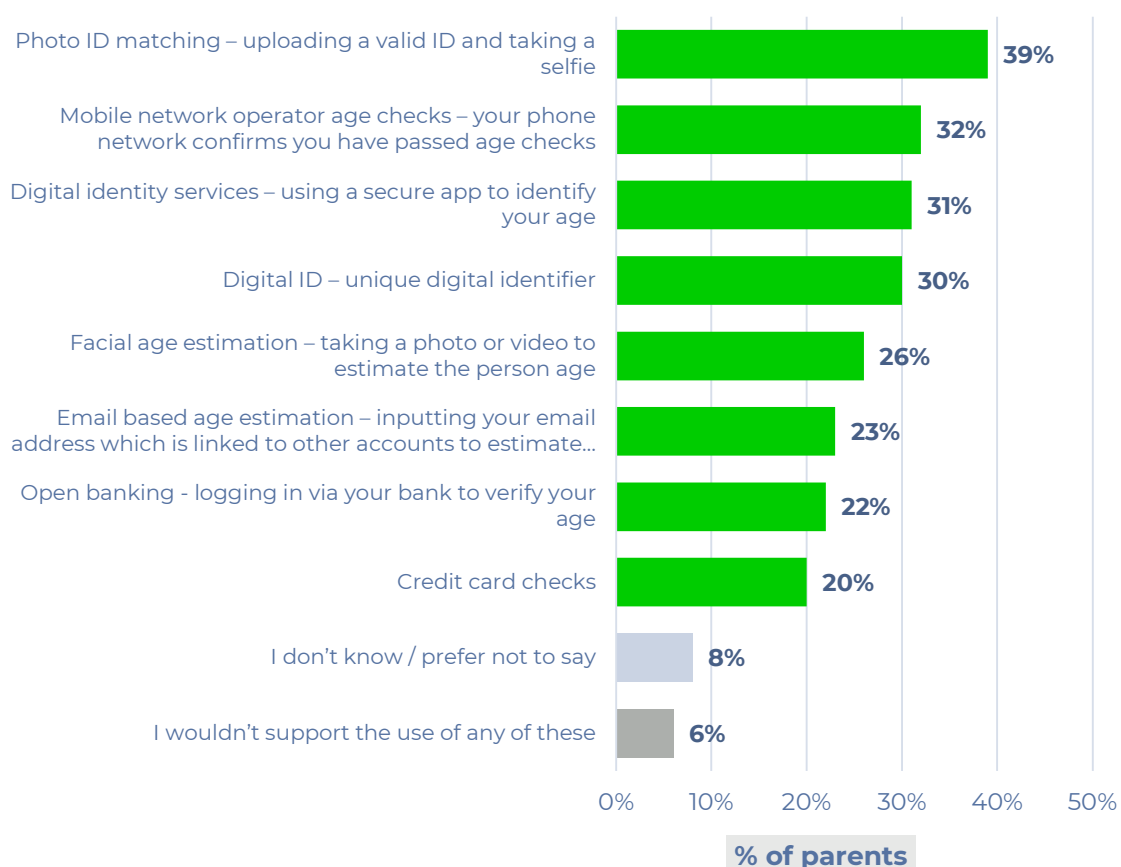
*Internet Matters Pulse* finds that parents favour parental approval beyond age 13 when children create accounts on social media platforms and other online services: 74% selected age 14 or above, with the most common responses being age 16 (36%), followed by age 17 (22%).<sup>101</sup>

Parents also appear willing to accept wider use of age checks where there is a clear child-safety purpose. *Internet Matters Pulse* finds that 80% of parents agree adults should complete age checks more often if this helps children access age-appropriate content and services, with only 6% disagreeing.<sup>102</sup> This suggests that

parents do not object to age assurance in principle, but it must be clearly linked to safer, age-appropriate experiences for children.

Parents are also open to a range of approaches that could support age verification (Figure 8). *Internet Matters Pulse* finds that parents support several possible methods for verifying age, including photo ID matching (39%), mobile network operator checks (32%), digital identity services (31%), digital ID (30%), facial age estimation (26%) and email-based age estimation (23%)<sup>103</sup>

**Figure 8. Age verification methods supported by parents**



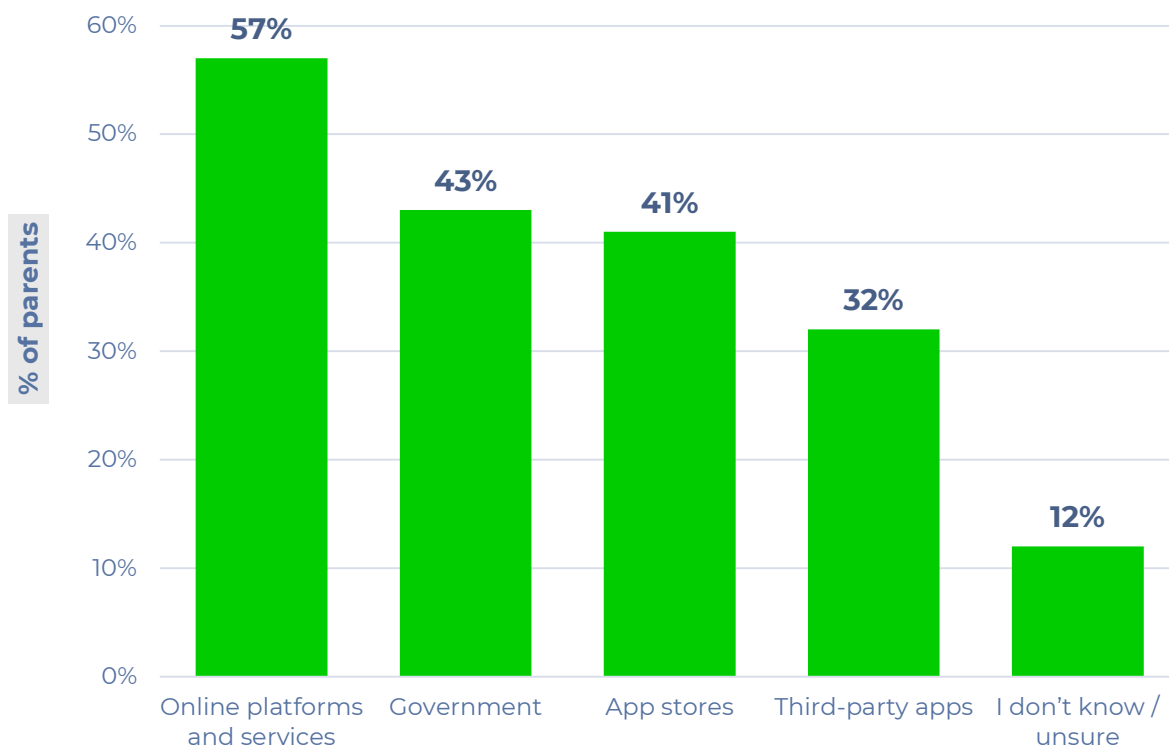
**Figure 8. Age verification methods supported by parents** | Data from *Internet Matters Pulse* (May 2026).  
Base: All parents (2000). Q: Which methods would you support the use of to verify your age online?

Any approach should therefore be practical for families, clearly explained and designed so that parents understand what role they are being asked to play.

Parents are also open to different approval routes for their involvement. *Internet Matters Pulse* finds that the method parents support include setting up the account with their child and verifying their identity where required (57%), email confirmation (52%), and logging in through a verified parent account, such as a linked family account (50%).<sup>104</sup> This suggests that parental approval needs to be practical and flexible, rather than dependent on a single method.

At the same time, parents do not see age verification as primarily their responsibility. *Internet Matters Pulse* finds that parents see online platforms and services as having the greatest responsibility for verifying age (57%), followed by Government (43%), app stores (40%) and third-party apps (32%) (Figure 9).<sup>105</sup>

**Figure 9. Responsibility for age verification to access online platforms and content**



**Figure 9. Responsibility for age verification to access online platforms and consent** | Data from *Internet Matters Pulse* (May 2026).

Base: All parents (2000). Q: Who should be responsible for verifying people's ages, including children's, to access content and platforms online?

However, parental approval will only be meaningful if the wider system works. If services rely on weak age checks or confusing approval processes, parents may be asked to approve access without clear information about what risks are involved or what protections are in place.

Government should therefore ensure that any parental approval system is easy to understand, consistent across services, privacy-preserving and accessible to different families. This includes families with different levels of digital confidence, documentation, language needs, caring arrangements and access to technology. Parents should not be asked to approve large numbers of unclear or inconsistent requests across every service their child uses.

Parental consent should not be treated as a substitute for safer defaults, age-appropriate design or platform accountability. Parents should be supported to

make informed decisions, but services should remain responsible for ensuring children are not exposed to age-inappropriate services, features or data practices.

### 3.6 Services should report on whether age assurance is effective in practice

Ofcom and Government should require services to show whether age assurance is working in practice. It is not enough for a service to say that it has introduced an age check. Services should be able to show whether children are being prevented from accessing age-inappropriate services and features, and whether child users are being moved into safer, age-appropriate experiences.

Services should report on which age assurance methods they use, what those methods are being used for, and how well they are working. This should include reporting on accuracy, false positives and false negatives, rates and methods of circumvention, complaints and appeals, user experience, and impacts on different groups of users.

Reporting should also cover whether age assurance applies to existing accounts, not only new sign-ups. Many children are already using services below stated minimum ages. Services should therefore be expected to identify and address underage existing accounts, not only prevent new underage access.

Services should also report on what happens after a user's age is established. This includes whether child users are moved into age-appropriate experiences, whether safer defaults are applied, whether high-risk features are restricted, and whether reporting and support routes are suitable for children.

Greater transparency would help Ofcom and Government assess whether age assurance is making children safer in practice. It would also help build public trust by showing how services use age information, what safeguards are in place, and whether children are better protected as a result.

### 3.7 What Government must do

Effective compliance and enforcement cannot depend on services simply introducing age checks. Government should focus on whether age assurance works in practice, whether children are moved into safer experiences, and whether services are accountable for the protections they provide. Government should therefore focus on:

- **Requiring services to use age assurance effectively.** Services should be required to use age assurance in ways that work in real-world conditions, including against common workarounds such as fake birthdates, shared accounts, shared devices, someone else's ID and repeated attempts after failed checks. Age information should also be used to apply safer defaults, content restrictions, feature limits, reporting routes and parental controls, not simply to block access.

- **Prioritising effective age assurance over VPN restrictions.** VPN use should be monitored, including whether children's use changes over time, but current evidence suggests VPNs are not the main route children use to bypass age checks. Government should focus first on improving the requirements on platforms age assurance systems and addressing common workarounds.
- **Making age assurance privacy-preserving and inclusive.** Government should require multiple routes, clear explanations, data minimisation, accessible appeals and safeguards against exclusion or bias.
- **Supporting parental involvement without shifting responsibility to parents.** Parents should be able to approve or support account creation where appropriate, but services must remain responsible for robust age assurance and safe design.
- **Requiring transparency and accountability.** Ofcom should require services to report on age assurance methods, purposes, accuracy, circumvention, complaints, appeals, user experience and outcomes for children, including across new and existing accounts.

A safer online environment for children will require more than setting age thresholds or introducing age checks. It will require services to show that age assurance is being used effectively, that children cannot easily bypass protections, and that age information leads to safer, age-appropriate experiences.

## Chapter 4: Preparing children for a digital future and enriching their online experiences

Alongside platforms protecting children from harm, families need the skills, knowledge, confidence and support to navigate digital environments safely and positively. Media literacy<sup>x</sup> can help children evaluate information, manage online interactions, understand platform design, protect their privacy, seek help and make the most of the benefits of being online. However, media literacy cannot replace safer service design, effective regulation or platform accountability.

Internet Matters' evidence shows that many children feel confident online, but still have gaps in the skills and knowledge needed to manage increasingly complex digital environments. Children are often more confident taking basic actions, such as blocking or reporting, than understanding the systems that shape what they see, who they interact with and how long they spend online. Parents also need practical support, particularly on age-appropriate services, parental controls, screen time and specific online safety issues.

This chapter argues that Government should treat media literacy as a core part of online safety implementation. This requires stronger leadership from Government, better support for schools, practical guidance for parents, media literacy-by-design from platforms, sustainable funding for civil society, and tailored support for children with additional needs.

### 4.1 Children and families need media literacy support that reflects the reality of online life

Children report relatively high levels of confidence in their ability to stay safe online. *Internet Matters Pulse* finds that 72% of children feel confident in knowing how to stay safe online, while only 20% report feeling unconfident.<sup>106</sup> However, our research finds that this confidence does not always reflect the depth of skills and knowledge needed to navigate increasingly complex digital environments.

The need for improved media literacy is reflected in the range of online harms children face (Figure 10). *Internet Matters Pulse* shows that three in four children (75%) encounter at least one online harm. These harms include encountering content risks, such as dangerous stunts or challenges (22%); harmful interactions with others, such as experiencing bullying, trolling or abuse (21%); and privacy and financial risks, including being asked to share or having shared personal

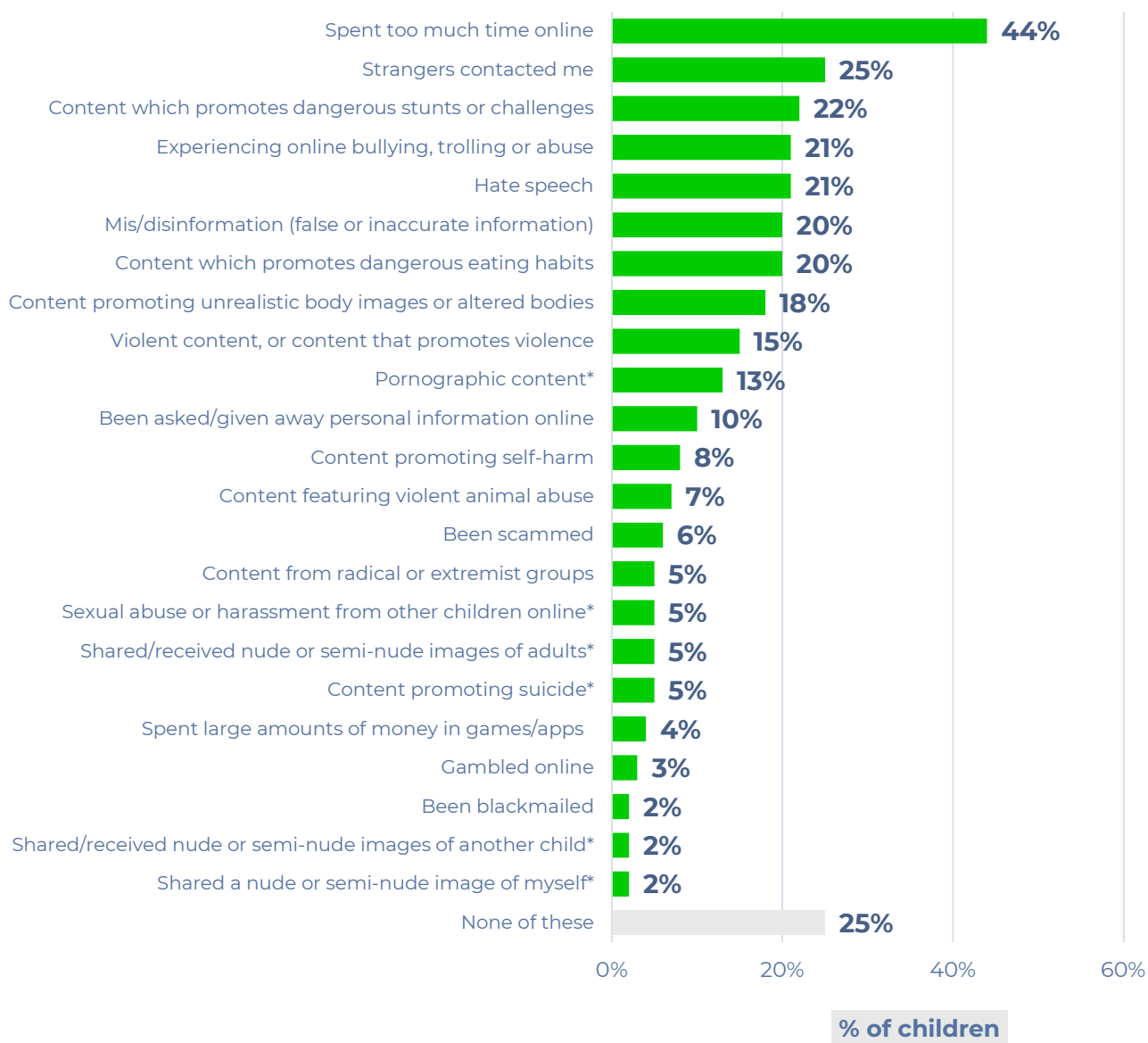
---

<sup>x</sup> DSIT's consultation distinguishes between "media literacy", focused on understanding, questioning and making sense of online content, and "digital literacy", focused on the practical skills needed to use devices and online services safely, confidently and independently. Internet Matters defines media literacy as: being able to evaluate information and distinguish between what is true and false online; being able to create and share digital content responsibly and safely; and the awareness and ability to protect yourself from the risks of being online.

information online (10%). Children also need support to manage their online habits, with 44% saying they spend too much time online.<sup>107</sup>

These findings show that media literacy must include a wide range of skills, including a focus on supporting children to manage time online, evaluate content, understand platform design, recognise harmful or manipulative information, manage contact with others, protect their personal and behavioural data, create and share content responsibly, understand financial risks, and know how and when to report or seek help.

**Figure 10. Children’s experience of harm online**



**Figure 10. Children’s experiences of harm online** | Data from Internet Matters Pulse (November 2025).  
 Base: All children (1000). Q. And which of the following have you experience online?  
 \*Only asked to children 13+. Base: Children 13-17 (574).

## 4.2 Children need support across specific areas of media literacy skills and knowledge

The media literacy topics identified in the Government's consultation are important, but they are broad and overlapping. Internet Matters' view is that Government should translate these broad topics into the practical skills and knowledge children need to navigate online life. This means helping children understand and evaluate the content they see; understand how services shape their experiences, including through algorithms, recommender systems and persuasive design; manage contact and interactions with others; protect their privacy and personal data; navigate sexual and gendered harms; and know where to go for help when something goes wrong. The sections below set out several of these priority areas in more detail.

### 4.2.1 Children need stronger skills to evaluate information and understand the role of AI

Children are increasingly required to evaluate a wide range of online content, including reliable information, misinformation, manipulated media and AI-generated content. This is becoming more difficult as synthetic and manipulated content becomes more realistic and more widely encountered across social media feeds, search engines, video-sharing platforms and other online spaces.

Media literacy support should help children and families understand how AI is increasingly built into the services children already use, including through AI-generated content, chatbots, recommender systems, search, personalisation and content moderation. This matters because children may encounter AI without actively choosing to use a standalone AI tool.

There are signs that children are receiving some support on AI, but this is not yet consistent or embedded. Just over half (57%) of children report having spoken with teachers or school about AI, while only 18% recall having had multiple conversations.<sup>108</sup> This suggests that children need more regular and structured opportunities to understand how AI works, where it appears in their online lives, and how to evaluate AI-generated or AI-shaped content.

*Internet Matters Pulse* shows that one in five (20%) children report coming across mis- or disinformation.<sup>109</sup> Our report on children's online news consumption finds that over a quarter (27%) of children have believed a fake or AI-generated story, while 41% think they may have done so.<sup>110</sup> We also find that only around half of young people aged 13-17 feel confident determining whether information they see online is true or false (53%), or distinguishing between fact and opinion online (59%).<sup>111</sup>

These skills matter because young people's ability to assess information can affect how they understand the world around them, including news, politics, health, relationships and social issues. For example, Internet Matters' research

finds that children's ability to evaluate political information online is linked to their confidence in engaging with it, which may in turn shape how they participate in civic and democratic life.<sup>112</sup>

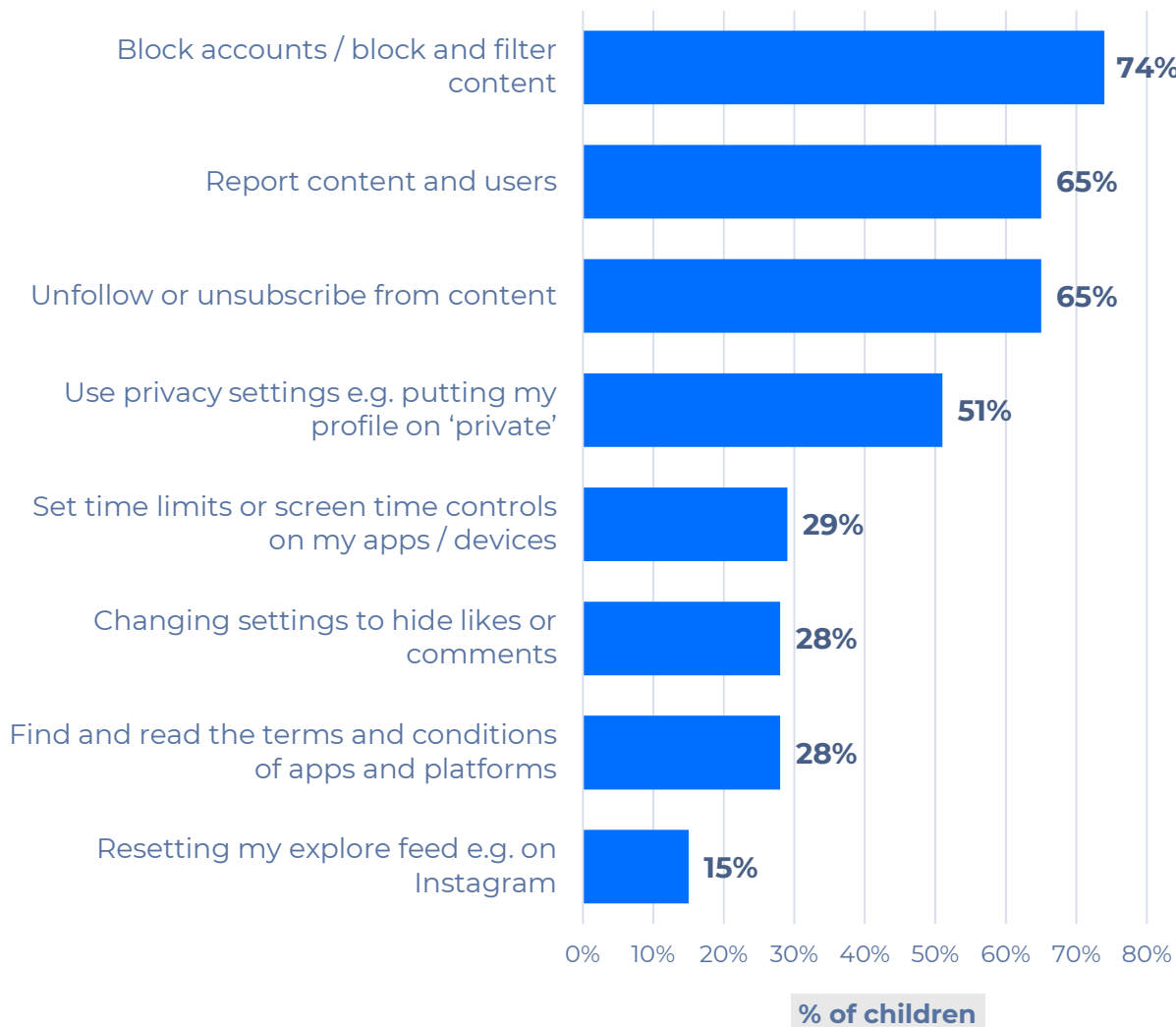
#### 4.2.2 Children need support to understand platform design and manage online habits

Children also need to understand how platforms shape what they see, how they interact and how long they spend online. Features such as recommender systems, infinite scroll, autoplay, notifications and engagement metrics influence children's online experiences, but can be difficult for children and families to see or understand.

This should also include support to understand how AI and other emerging technologies are being built into online services, including through personalisation, recommender systems, content moderation and automated decision-making. Teaching children and families how these technologies work can help them recognise and manage risks in the gap between new technologies emerging and regulation catching up.

*Internet Matters Pulse* shows that while many children are confident using basic platform tools, this capability is uneven and often limited to straightforward, reactive actions that are easy to find in-platform (Figure 11). A majority report knowing how to block accounts and block or filter content (74%) and report users and content (65%). However, fewer children know how to take more advanced or preventative actions, such as setting screen time controls (29%), changing settings to hide likes or comments (28%), or reset content feeds (15%).<sup>113</sup>

**Figure 11. Children’s knowledge of actions to keep them safe online**



**Figure 11. Children’s knowledge of actions to keep them safe online** | Data from [Internet Matters Pulse](#) (November 2025).  
 Base: All children (1000). Q: Which of the following do you know how to do?

This suggests that children are often better equipped to respond to issues once they arise than to understand or manage the systems that shape their online experiences. Media literacy support should therefore help children and families understand how platforms work. This includes understanding algorithms and recommender systems, persuasive design, privacy and account settings, reporting and redress, and how to manage content feeds and screen time controls.

Screen time is a particular area where children and parents need practical support, as outlined in Chapter 2. Among other negative outcomes, spending a lot of time online can affect children’s physical health: 63% of parents say that spending a lot of time online affects their child's physical health, such as straining their eyes, making them tired or unable to concentrate and affecting their

posture, while one in three (29%) children self-report this.<sup>114</sup> Support should not focus only on how much time children spend online, but also on the design features and habits that make it difficult to disengage.

#### 4.2.3 Children need support to manage privacy, contact and online interactions

Children require support to manage risks related to privacy, contact and online interactions. *Internet Matters Pulse* finds that 25% of children report being contacted by strangers, while 10% report having been asked to share or having shared personal information online. Children also report experiencing online bullying, trolling or abuse (21%).<sup>115</sup>

These risks highlight the importance of ensuring that children understand how to protect their information, recognise potentially harmful interactions, and make informed decisions about who they engage with online. Support should include using privacy settings, recognising suspicious contact, understanding age-appropriate services, reporting harmful content, blocking users and knowing when to seek help.

This is not only about technical knowledge. Children also need broader skills related to communication, judgement and emotional resilience, including recognising the impact of their own behaviour and understanding how online interactions can escalate or cause harm. This includes support to be able to create and share content responsibly.

#### 4.2.4 Children need support on sexual image sharing, pornography, misogyny and gendered harms

Government should also consider the need for stronger support on sexual image sharing, pornography, misogyny and gendered harms. These are not only online safety issues, but also media literacy issues: children need support to understand consent, pressure, harmful norms, gendered abuse and how online content and interactions can shape expectations about relationships, bodies and behaviour.

Internet Matters' research on online misogyny and image-based abuse found that 11% of teenagers aged 13-16 had been sent a nude photo or video by someone, with 14% saying someone they knew had experienced it. When asked about it, 81% of teenagers aged 13-16 think sharing nude images is always harmful.<sup>116</sup>

In our research into the prevention of sexual image-sharing, children told us that the biggest barrier to effective education on nude image-sharing was in the implementation of PSHE lessons. Girls in particular told us they wanted resources to acknowledge the core differences in their experience of sexual image-sharing compared to boys – namely that boys were more likely to perpetrate and pressure girls for images while girls are more likely to experience harassment for those images. Children also spoke positively about the impact of nudges on platforms at point of upload as a preventative measure.<sup>117</sup> Our research also

suggests that children are more likely to receive lessons on less sensitive topics like password security than more difficult topics like image-sharing – further highlighting the need to support schools with this topic.<sup>118</sup>

Parents also need support to have these conversations in ways that are practical, non-judgemental and grounded in children’s real experiences. Guidance should help parents talk to children about consent, pressure, image sharing, pornography and misogyny without relying on shame or fear, and should clearly signpost where families can go for help when something has gone wrong.

### **4.3 Schools are essential, but need training, resources and support**

Schools are the primary mechanism through which children can develop media and digital literacy at scale. They are a consistent and trusted institution in children’s lives.

Children and parents also value the role schools can play. *Internet Matters Pulse* finds that 65% of children and 49% of parents get their information about how to stay safe online from schools.<sup>119</sup> This makes schools an important route for reaching families with online safety and media literacy support.

However, there are well-established challenges in how effectively media literacy education is currently delivered in schools. As set out in *Internet Matters’ A Vision for Media Literacy*, evidence shows variation in both the quality and consistency of provision, with some schools delivering strong, integrated approaches while others provide more limited or ad hoc teaching.<sup>120</sup> Teachers often report low confidence in delivering media literacy, reflecting gaps in training, unclear guidance and limited access to high-quality, up-to-date resources.

This inconsistency in media literacy provision is also reflected in children’s experiences. *Internet Matters’ Informed or Overwhelmed?* finds that only 56% of children and young people across the UK who consume news report that their school or teacher has spoken to them about how to tell whether online news is true. Only one in five (20%) report that their school has had multiple conversations about online news verification. Access also varies by socioeconomic background, with children in higher income households more likely to report having these conversations than those in lower income households (66% compared to 46%).<sup>121</sup> This echoes our research on AI chatbots, which found that only 57% of children across the UK report having had conversations with teachers or school about AI.<sup>122</sup>

We welcome the Government’s recent commitment, following the Curriculum and Assessment Review, to embed media and digital literacy more clearly across the English school curriculum.<sup>123</sup> These reforms represent an important step towards addressing longstanding structural issues including what to teach and where. However, there is currently limited detail on how the existing challenges

faced by teachers - including gaps in training, guidance and access to high-quality resources - will be addressed.

While curriculum reform is a devolved matter, the issues raised in this consultation are relevant to children and families across the UK. Government should therefore consider how best to share the findings from this consultation with education departments across all devolved nations, so that media and digital literacy support can be informed by a common understanding of children's online experiences, while respecting differences in education policy and delivery across the UK.

To support effective rollout, Government should create a clear, easy-to-access repository of relevant resources to teach media and digital literacy. This should be kept up to date with emerging threats and trends so that teachers can access resources that keep children engaged and prepare them to participate safely in changing online spaces.

These resources should be developed alongside technology companies and third sector organisations, who are well placed to support learning and ensure that emerging trends and threats are reflected in the development of new resources. Resources should be suitable for a range of learners, with specific resources developed for children with additional needs. They should also include materials that can be delivered with and actively reinforced by parents. Government should also ensure there are options for teachers who, due to limited resources, need to teach media literacy through non-digital or semi-digital environments, such as classrooms with shared laptops or limited internet access.

Government should ensure that all teachers across the UK are trained in media literacy education, through both initial teacher training and ongoing professional development. This training should address the changing nature of technologies, threats and online life. Schools across the UK should also be provided with clear guidance on how, when and where to teach the full range of media literacy topics.

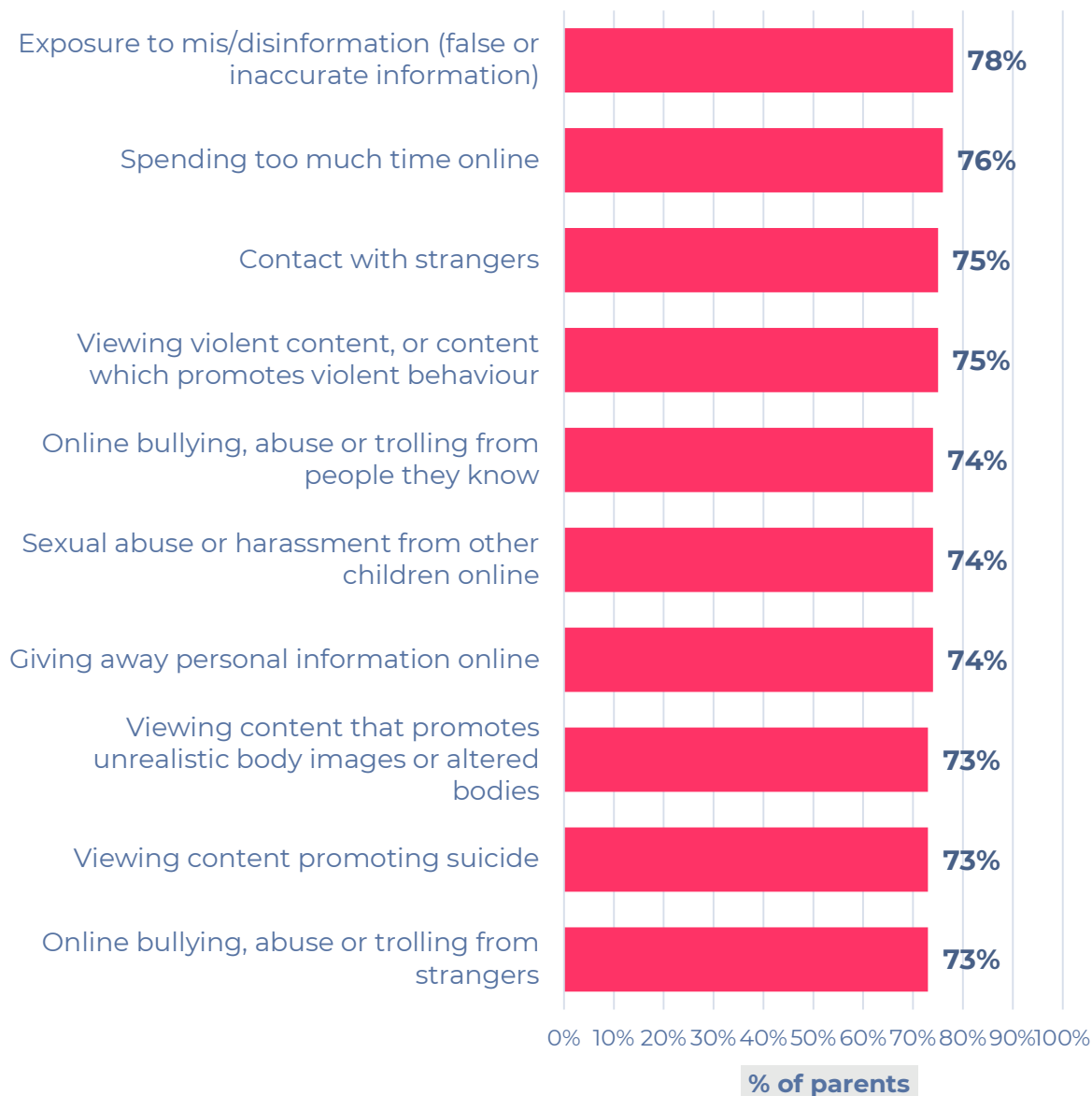
There is also a question of timing. The revised school curriculum in England is not expected to be implemented until 2028, meaning that many children will continue to move through the education system without benefiting from these improvements. Government should therefore set out what support will be available before the revised curriculum is implemented, including teacher training, guidance, quality-assured resources and support for schools to respond to emerging risks such as AI-generated content, misogyny and harmful platform design.

#### **4.4 Parents and carers need practical support to help children navigate online risks**

Parents and carers play a central role in supporting children’s online safety, so it is important to support their media literacy alongside that of their children. Most children (85%) report that they get information about how to stay safe online from their parents or carers.<sup>124</sup> However, parents themselves report high levels of concern about a wide range of online risks (Figure 12).

*Internet Matters Pulse* finds that parents’ highest areas of concern include mis- and disinformation (78%), spending too much time online (76%) and contact with strangers (75%). These concerns broadly mirror the range of risks children report experiencing, reinforcing the need for practical support for families.<sup>125</sup>

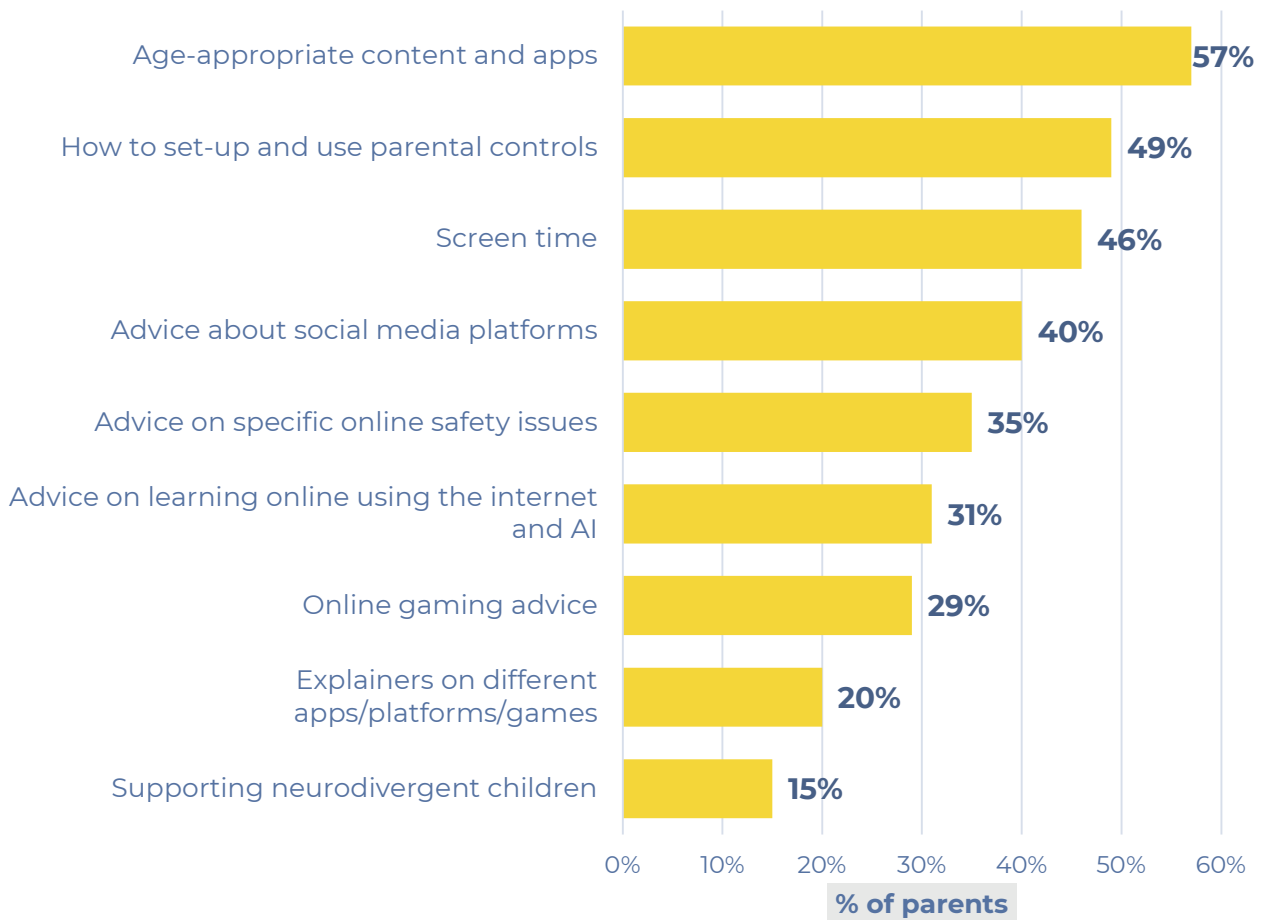
**Figure 12. Parents' top concerns about their children's online lives**



**Figure 12. Parents' top concerns about their children's online lives** | Data from *Internet Matters Pulse* (November 2025).  
 Base: All parents (2000). Q. How concerned, if at all, do you feel about any of the following issues in relation to your child / children's online experience? [NET: Concerned – Very concerned & Somewhat concerned]

Parents' information needs also show where support is most needed. *Internet Matters Pulse* finds that parents are most interested in information about age-appropriate content and apps (57%), setting up and using parental controls (49%), screen time (46%), social media platforms (40%) and specific online safety issues (35%) (Figure 13).<sup>126</sup> Screen time is a particular area where parents want practical support, with 72% agreeing Government should give parents advice on how much screen time is suitable for children aged 5–16.<sup>127</sup>

**Figure 13. Online safety information parents are interested in**



**Figure 13. Online safety information parents are interested in** | Data from [Internet Matters Pulse](#) (November 2025).  
Base: All parents (2000). Q. *What information related to children's online safety are you most interested in?*

These findings show that families need clear, practical and accessible guidance across a broad range of topics. This should not only explain risks, but help parents and carers take action: choosing age-appropriate services, setting up parental controls, managing screen time, understanding platform features, talking to children about online experiences, and knowing where to go for support when something goes wrong.

Support should be delivered through multiple routes, including schools, Best Start family hubs, the Government's online safety hub, platforms, public campaigns and third sector organisations like Internet Matters. This will require increased and sustained funding for organisations that conduct research, produce guidance and reach families with practical support.

Parents should also be better engaged in media literacy education. Schools are already skilled in building partnerships with parents in other areas where parental input is key – for example, encouraging younger children to read or supporting healthy eating. The same principle applies to supporting children in

their online lives. At present, many parents do not feel engaged in or knowledgeable about their children's school's media literacy teaching.<sup>128</sup>

Government should support schools to engage parents more actively on media literacy and online safety. Internet Matters finds that the school-home relationship is particularly important because children most commonly turn to parents and teachers for information about how to stay safe online. However, outreach is currently uneven. While three-quarters (75%) of parents had experienced at least one form of school outreach on online safety, only 15% had attended an event or session hosted by the school. This matters because events and sessions appear to have the greatest impact: 80% of parents who had attended one said it made them somewhat or a lot more confident about keeping their child safe online. Other forms of outreach were also valued, including receiving information about how the school plans to teach children about online safety (73%), reading the online safety section of the school's policies (68%), and receiving information from school about how to keep children safe online (68%).<sup>129</sup>

Schools should therefore be supported to use a mix of approaches to engage parents, rather than relying only on sending information home. This could include explaining how online safety and media literacy are taught, making online safety policies accessible to parents, signposting trusted resources, and offering opportunities for parents to discuss practical issues such as parental controls, age-appropriate services, screen time, social media, sexual image sharing and responding when something goes wrong.

#### **4.5 Media literacy should be built into online services by design**

Online services have an important role to play in supporting media literacy. Media literacy should be embedded into the design of digital services, through features that help users evaluate, question and contextualise the content they encounter.

This could include clearer labelling of AI-generated or manipulated content, prompts that encourage users to reflect before sharing, and specific interventions when a platform detects a nude image or video being uploaded.

Platforms should also offer support to help users understand how services, features and functionalities work. This includes clear prompts and guidance on how to report content, block users, change privacy settings, and understand why these actions are important. Platforms should also provide greater transparency and control over how content is recommended and presented, including clearer information about algorithms and recommender systems.

In addition, platforms should share or signpost trusted resources and support, particularly where children or families are seeking help or responding to harmful or upsetting experiences, and during crisis events. Platforms should also make it

clearer how parents can manage and support their children's experiences while they use their services.

These interventions should be designed to reach children directly, as well as through parents and carers. Some children may not have a parent or carer who is able to support them consistently, while others may be more likely to seek help from teachers, youth workers, trusted professionals or specialist organisations. Platform-based support should therefore include child-facing guidance, accessible reporting routes and trusted signposting to appropriate sources of help, not only information aimed at parents.

Technology companies should collect data on the effectiveness of on-platform media literacy-by-design interventions and publish evaluation data to inform the wider media literacy sector. This would help build the evidence base on what works and support more consistent implementation across industry.

Strong, effective media literacy-by-design across industry could be achieved through a legally binding set of principles that platforms are required to follow. If these principles are delivered only through guidance, there is a risk that platforms will not adopt them consistently or at sufficient scale.

#### **4.6 Civil society needs sustainable funding to provide trusted support**

Civil society organisations play an important role in providing trusted, accessible and specialist support for children and families. They are often well placed to meet the needs of different communities, including children with additional needs. *Internet Matters Pulse* finds that 42% of parents use online safety organisations to find online safety information.<sup>130</sup>

The value of this role is reflected in evaluation of Internet Matters online resources, which received over 3 million UK visitors last year. Among parents who have used the Internet Matters website, 95% say it gives practical steps they can take to help keep their child safe online. Importantly, parents also report taking practical action after visiting the website: 41% set up parental controls on their child's devices, 50% talked to their child about being safe online more frequently and 44% reviewed their child's online safety settings in privacy settings or on social media.<sup>131</sup> This demonstrates the value of trusted third sector organisations in reaching families and supporting practical behaviour change.

To date, government efforts to support and fund civil society have suffered from a lack of strategic priority and long-term, sustained funding. Pilots are typically piecemeal and often lack follow-on funding. This restricts the ability of media literacy organisations to robustly evaluate projects and coordinate efforts and learnings.

Government should consider how this work is sustainably funded and coordinated, including whether mechanisms such as a levy on technology

companies could support investment in media literacy initiatives, specialist resources and public awareness campaigns.

#### **4.7 Children should be able to find high-quality, age-appropriate online content**

Children should have access to high-quality online content that supports their wellbeing, learning, creativity, connection and participation. The online world should not only be made safer by reducing children's exposure to harmful content; it should also help children find content that is reliable, enriching and appropriate for their age and stage of development.

Government should work with trusted experts to define what is meant by high-quality, age-appropriate online content for children. This should include children, parents, educators, child development experts, child advocacy organisations and age-rating or classification experts. Any definition should consider content that supports children's learning, creativity, civic participation, emotional wellbeing and access to reliable information, while recognising that children's needs will vary by age, maturity, ability, background and vulnerability.

The BBC Charter Review provides an important opportunity to consider the role of public service media in supporting children's access to trusted, enriching and age-appropriate content, and in helping to define what "high-quality online content" looks like in practice. Trusted public service and classification bodies, including the BBC and the British Board of Film Classification (BBFC), may have an important role to play in shaping standards and helping families identify content that is reliable, enriching and suitable for children.

Any government intervention should focus both on ensuring that high-quality and age-appropriate content exists, and that children and families can find it. High-quality content will not benefit children if platform design, recommender systems or search rankings make it difficult to discover. Government should therefore consider whether platforms should be expected to help surface reliable, age-appropriate and enriching content through search, recommender systems, labelling, trusted signposting and user controls.

This would also support parents and carers. Parents are often expected to judge whether content, services and features are suitable for their child, but this is difficult in a fast-moving online environment where content is personalised, algorithmically recommended and inconsistently labelled. Clearer standards, trusted labelling and better surfacing of age-appropriate content would help parents feel more confident identifying high-quality content and making informed decisions about the platforms and services their child uses.

Recent polling from the BBFC also suggests strong parental support for trusted classification approaches being applied to social media. The BBFC found that almost nine in ten (86%) parents would support a formal partnership between the

BBFC and social media platforms, where social media content would be moderated in line with the same BBFC classification standards used for UK cinemas. Nearly three-quarters (73%) would be more likely to let their child use social media if content was moderated in line with these standards. Government should therefore consider how trusted classification approaches, labelling and platform design can support families to make more informed decisions about children's online experiences.<sup>132</sup>

This should not be left to voluntary action alone. Voluntary approaches are unlikely to be adopted consistently or at sufficient scale, particularly where surfacing high-quality, age-appropriate content may conflict with engagement-driven business models. Government should therefore consider what expectations should be placed on platforms that are accessed by children, so that children are not only protected from harmful content, but actively supported to find reliable, enriching and age-appropriate content.

High-quality content should also reflect different children's needs and experiences. Content should be accessible, inclusive and relevant for children of different ages, abilities, backgrounds and vulnerabilities, including children with additional needs. This matters because children will not benefit equally from high-quality content if it is not designed, labelled, recommended or presented in ways that meet their needs

## **4.8 Children with additional needs need tailored and accessible support**

### **4.8.1 Children with additional needs experience online life differently**

As set out in Chapter 1, children with additional needs often experience more of the benefits and harms of online life than their peers.<sup>xi</sup> For example, the *DWI Year 5* finds that a rising number of children report spending large sums of money in games or apps, with this trend more pronounced among children with additional needs (13% c.f. 9% of all children). Parents of children with additional needs are also more likely to report that their child spends money in apps or games without realising (47% c.f. 23% of parents of children without these needs).<sup>133</sup>

These children are also more likely to struggle to regulate their time online: 34% of children with additional needs feel they cannot control how much time they spend online, compared to 25% of children without additional needs.<sup>134</sup> Children with additional needs are also more likely to post things they later regret, with 22% doing so compared to 12% of children without additional needs.<sup>135</sup>

Children with additional needs also often experience and understand digital environments differently, creating additional challenges when engaging online.

---

<sup>xi</sup>We refer to children who have an Education, Health and Care Plan (EHCP), who receive special educational needs (SEN) support, or who have a physical/mental health condition which requires professional help as having additional needs. There are an estimated 2 million children with additional needs across the UK.

Internet Matters' report *More than a Game* finds that some neurodivergent children report difficulties with aspects of digital engagement, including sensory experiences (27%), accessibility (23%) and communicating with others online (22%).<sup>136</sup> These findings suggest that media literacy support for children with additional needs should not only cover online risks, but also help children navigate the practical, social and sensory aspects of digital spaces.

#### 4.8.2 Media literacy support should be tailored for children with additional needs

Children with additional needs also show less improvement over time in some key skills. For example, the *DWI Year 4* finds that the proportion of children without additional needs who say they understand what information they should and should not share online has increased from 76% to 82% over the past three years, compared to a much smaller increase from 70% to 71% among children with additional needs.<sup>137</sup> This suggests that, without tailored support, some children may be less likely to benefit from improvements in general online safety knowledge and skills.

Children with additional needs need support across the same broad areas of media literacy as other children, but this support should be delivered in ways that are more accessible, practical, repeated and tailored to the specific risks they are more likely to encounter. This includes understanding limits on privacy and personal information sharing; recognising harmful contact or behaviour; navigating social cues and peer pressure online; managing spending in games and apps; understanding persuasive design features and regulating screen time; recognising sexual pressure, image-sharing risks and coercive behaviour; and knowing when and how to seek help.

Support should be co-designed with children with additional needs and their parents and carers, with input from specialists such as SEND professionals, child development experts and organisations that work directly with these families. This would help ensure resources are practical, accessible and grounded in children's real experiences.

#### 4.8.3 Parents of children with additional needs need specialist and accessible support

Parents and carers of children with additional needs also require tailored support. *Internet Matters Pulse* finds that parents of children with additional needs are most likely to get information about keeping their child safe online from schools or teachers (51%), followed by looking up information online themselves (49%). By contrast, parents of children without additional needs are most likely to look up information online themselves (60%), followed by schools or teachers (49%).<sup>138</sup> Parents of children with additional needs are also more likely than other parents to use online safety organisations for information (48% compared with 40%). This suggests that support for these families should not rely only on general online

guidance but should also be available through schools and specialist organisations.<sup>139</sup>

Support should also reflect the specific environments where children with additional needs may be spending time or deriving particular value, including gaming services<sup>140</sup> and AI chatbots<sup>141</sup>. In these contexts, parents may need practical guidance on social interaction, spending, persuasive design, privacy, contact from unknown users, and the risks of emotionally responsive or personalised AI systems.

Their concerns also differ from those of parents of children without additional needs in important ways. For example, parents of children with additional needs are more likely to be concerned about their child gambling online (63% c.f. 49% of parents of children without additional needs), spending large amounts of money in games or apps (66% c.f. 56%), sharing nude or semi-nude images of themselves (73% c.f. 64%), being blackmailed (71% c.f. 63%), and sharing or receiving nude or semi-nude images of other children (74% c.f. 67%).<sup>142</sup>

These findings suggest that support for families of children with additional needs should reflect the specific risks they are most concerned about, and should be available through multiple trusted routes, including schools, specialist organisations and accessible online resources.

When it comes to actions parents take to manage their children's online lives, we find that there are key differences relating to managing time spent online. Parents of children with additional needs are less likely to have clear rules about how much time they can spend online (41% c.f. 52%) and are less likely to take devices away at certain times (29% c.f. 39%).<sup>143</sup> This echoes previous research, which found that parents of children with additional needs find it harder to set boundaries with their children about their online lives due to the fact that online spaces often play a more prominent and important role in these children's lives.<sup>144</sup>

Tailored support is therefore not just about adapting the format of guidance. It is about ensuring that advice reflects the specific risks, platforms and situations that children with additional needs and their families are navigating. This has implications for how resources are designed, who delivers them, and how easily families can access them.

#### 4.8.4 The role of supporting organisations

Internet Matters has sought to reflect these principles in its own evidence-based resources for parents and carers, which we develop to support children's online safety and wellbeing. This includes a dedicated hub for parents of neurodivergent children, and we are building a broader hub for parents of children with

additional needs.<sup>xii</sup> These resources are informed by our research with parents of children with additional needs and evaluation of previous resources, alongside engagement with the wider sector. This allows us to ensure content is accessible, practical and relevant. This includes using clear and simple language, offering guidance in a range of formats (such as text, visual and video content), and providing flexible, easy-to-use resources that parents and carers can access when needed.

Government should include tailored support for parents of children with additional needs in its online safety parent hub.<sup>145</sup> This should include advice and guidance relating to the harms we know children with additional needs are particularly at risk of, and which recognises the different dynamics at play for such children. This should include advice on contact from strangers, bullying and recognising mis- and disinformation, as well as guidance and support to help parents manage screentime. To avoid duplication of efforts, the hub should also signpost parents to existing, proven resources.

Teacher training should also include support for teaching children with additional needs about media literacy. This must include teaching assistants, classroom assistants and pupil support workers, who often support children with additional needs in educational settings. Training should help staff adapt resources to match children's individual needs.

Platforms should also design features and functionalities with children with additional needs in mind. This means ensuring that services can be tailored to children's ages and stages of development, and that settings and controls are easy for children and parents to understand and use.

#### 4.9 What Government must do

Media literacy cannot be a substitute for safer design or effective regulation. However, when delivered well, it can help children and families understand, question and navigate the digital environments they use every day. It can also support families to stay safe when regulation lags behind. Government should therefore treat media literacy as a core part of online safety implementation, not an optional education add-on.

Government should focus on:

- **Supporting schools to deliver media literacy consistently.** Government should provide clear guidance on what to teach and when, and how to engage parents in media literacy education. Government should also provide teacher training and an accessible high-quality repository of up-to-

---

<sup>xii</sup> Internet Matters' hub, *Supporting neurodivergent children & young people*, can be accessed here: <https://www.internetmatters.org/advice/neurodivergent-children/>

date resources for teachers. This should include interim support before school curriculum reforms are implemented in 2028 in England.

- **Providing practical support for parents, carers and children.** Government should ensure families can access clear, practical guidance on age-appropriate services, parental controls, screen time and specific online safety issues. Support should reflect the needs of both parents and children, and should link to relevant organisations such as Internet Matters to avoid duplication.
- **Supporting access to high-quality and age-appropriate content online.** Government should work with trusted experts to define high-quality and age-appropriate content for children, and consider how trusted classification, public service media and platform design can help families identify suitable content and help children find reliable, enriching content online.
- **Tailoring support for children with additional needs.** Government, schools, platforms and civil society should ensure that media literacy support is accessible, practical and tailored to the different risks and experiences of children with additional needs.
- **Providing clear leadership and accountability.** Government should build on the Media Literacy Action Plan by setting out defined roles and responsibilities, a clear approach to delivery, cross-government coordination, sustainable funding, and robust mechanisms for measuring progress and identifying gaps over time. This should include coordinating media literacy activity across Government, Ofcom, the Information Commissioner's Office (ICO), the Electoral Commission (EC) and other relevant bodies, so that efforts are aligned and mutually reinforcing.
- **Evidenced-informed media literacy interventions:** Government should evaluate what is working to improve children's online safety and fund interventions based on evidence. This could include a public campaign targeted at parents, building on the Government's recent pilot in Yorkshire, and could be linked to a national moment such as Safer Internet Day or a dedicated media literacy week.
- **Funding civil society sustainably.** Government should provide long-term funding for trusted organisations that support children and families.
- **Embedding media literacy into service design.** Government should require platforms to support media literacy-by-design. This can take many forms including labelling content, prompts, explanations, user controls, reporting guidance, trusted signposting and transparency over recommender systems. Government should consider legally binding principles to ensure consistent implementation.

Effective media literacy requires coordinated action across education, online safety regulation, platform design and family support. Without clearer leadership,

sustainable funding and stronger accountability, there is a risk that current efforts remain fragmented and fail to support children and families at the scale required.

## Chapter 5: Supporting families

Parents and carers play a central role in supporting children's online safety, but they cannot be expected to manage children's online experiences alone. Government should support families through clear, age-appropriate guidance on issues such as account settings, reporting routes and screen time, alongside practical tools such as parental controls. This support must sit alongside platform regulation that reduces the burden on parents.

This chapter sets out how parental involvement should change with children's age, maturity, development and needs; why families need clearer guidance on screen time and healthy digital habits; and how parental controls can be made easier, clearer and more consistent.

### 5.1 Parents provide a range of support, not just implementing technical controls

Internet Matters strongly supports parents having meaningful control over children's online experiences. Parents and carers play a central role in children's online safety: 85% of children say they get information about how to stay safe online from their parents or guardians,<sup>146</sup> and 69% of parents agree that it should be their choice if and when their child uses social media platforms and apps.<sup>147</sup> Meaningful parental control includes the ability to make decisions about services and features, set boundaries, advise children, talk to them about online risks, and help them respond when something goes wrong online.

Internet Matters' research shows that parents already play this role in several ways. When children report online harm, the most common action is for a parent or guardian to help them report it to the platform, with 58% saying this had happened; a further 38% say they or their parent/guardian reported the issue to a reporting support website, such as Report Remove or Report Harmful Content.<sup>148</sup> Parents and children also talk regularly about online safety: 50% of children say they have spoken to their parents or carers about online safety in the last month, and a further 23% say they have done so in the last two or three months.<sup>xiii</sup> These conversations cover a broad range of issues, including contact with strangers, spending too much time online, fake news and misinformation, online bullying, scams, privacy and personal information, and spending money online.<sup>149</sup>

Parents therefore need support to carry out all these roles effectively, including practical tools, trusted information and support to have informed conversations with children, understand how services work and know where to go for help when something goes wrong.

---

<sup>xiii</sup> As the survey was conducted in a two week period in October – November 2025, 'last two or three months' refers to the time before this period.

## 5.2 Parental involvement should change with age and need

Parental control should be flexible and responsive to children's age, maturity, development, needs and the risks they face. The level of control should gradually shift as children get older: younger children are likely to need stronger default protections and more managed parental oversight, while older children may need more autonomy, alongside guidance, discussion and support. Parents should also retain the ability to provide more tailored or sustained support where children have additional needs, vulnerabilities or face heightened risks.

Parents' approaches already change with children's age and stage of development. In Internet Matters' research on families' experiences under the Online Safety Act, parents of younger children focused more on parental controls and monitoring, while parents of older teenagers placed greater emphasis on trust and communication. This is also reflected in how parents describe their use of technical tools. Among parents who are aware of parental controls or technical tools but do not use them because they feel they do not need them, parents of older children are more likely to say they trust their child online or that their child is old enough not to need that level of restriction. For example, 56% of parents of 14-17-year-olds in this group say they trust their child online, and 60% say their child is older so does not need that level of restriction. By contrast, parents of younger children aged 3-10 are more likely to say they check their child's online use themselves (47% of parents of children aged 3-10 compared to 25% of parents 14-17) or limit which apps and platforms they use (35% of parents compared to 7% of parents of children aged 14-17).<sup>150</sup>

Government and industry should reflect this in the support and tools available to families. Younger children should have stronger default protections and parents should have access to more controls and oversight. This could include default parental controls, child accounts, restrictions on contact from unknown users, limits on spending, safer search and content settings, and clear prompts for parents when a child accesses a new service or feature. These protections should be easy for parents to understand and should not rely on parents manually finding and activating every setting. For older children, parental involvement should increasingly support shared decision-making, transparency and trust.

This does not mean parental involvement should fall away at 13. Children's online experiences remain complex throughout the teenage years, and older children can still face risks. For example, *Internet Matters Pulse* finds that nearly one in five (17%) of 16-17-year-olds say they have been contacted by a stranger in the last 12 months, and 27% have come across mis- or disinformation in the last 12 months.<sup>151</sup> Furthermore, as discussed in Chapter 3, *Internet Matters Pulse* finds that many parents want oversight to continue into the teenage years: 36% say children

should no longer require parental or carer approval to create an account at age 16, and 26% say this should be at age 17.<sup>152</sup>

Age should not be the only factor shaping parental controls and support. As explored in Chapter 4, some children, including those with additional needs or vulnerabilities, may need more tailored or sustained support, including into the teenage years, depending on their needs, maturity and the risks they face. This means controls should be flexible enough to adapt over time and to reflect children's individual circumstances, rather than assuming that all children need the same level of support at the same age.

### **5.3 Families need clearer guidance on screen time and healthy digital habits**

We welcome the Government's intention to develop screen time guidance for parents and carers of children aged 5-16. Families consistently tell us that managing time online is one of the most difficult aspects of digital parenting. *Internet Matters Pulse* finds that three-quarters (72%) of parents say the Government should give parents advice on how much screen time is suitable for children aged 5-16.<sup>153</sup>

However, guidance must avoid presenting screen time as a simple question of "hours online". Children's online experiences vary significantly depending on what they are doing, who they are interacting with, how they feel during and after use, and what online activity may be displacing. Time spent learning, creating, communicating with family or accessing support is different from time spent compulsively scrolling, encountering harmful content, or being kept online by persuasive design features.

Screen time guidance should therefore help parents think about the quality, context and impact of children's online experiences, not only the quantity of time spent online. It should support parents to consider how online activity affects sleep, mood, concentration, physical activity, family time, friendships and schoolwork, while recognising that online spaces can also play a positive role in children's learning, creativity and connection.

Guidance should also be age- and situation-appropriate. For younger children, parents may need clearer advice on routines, boundaries, device set-up and content choices. For older children, guidance should increasingly support conversations about sleep, mood, concentration, social comparison, persuasive design, misinformation, and how to build healthy habits. Advice should also highlight the needs of different families, for example, children with additional needs may rely more heavily on digital access for everyday tasks, friendship or learning.

Government should ensure that any screen time guidance is practical, non-judgemental and accessible to families with different levels of confidence and resource. It should also recognise that parents cannot address screen time

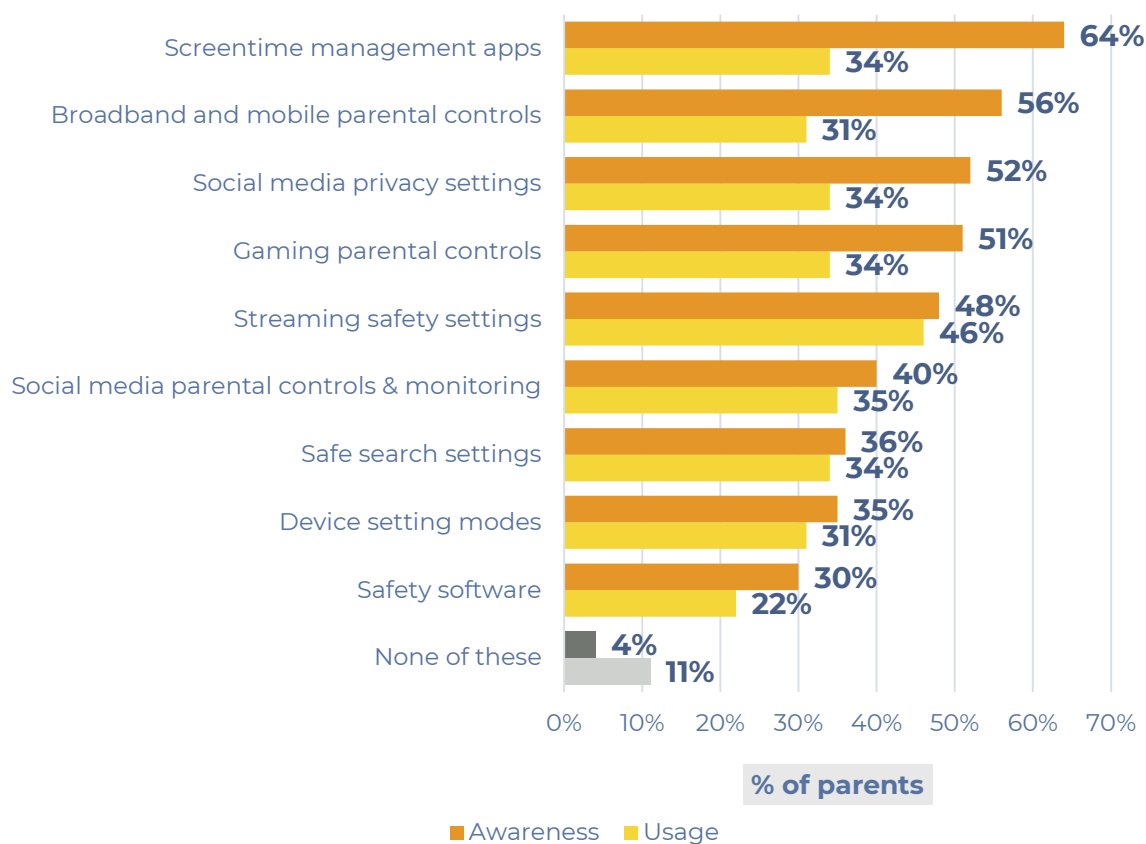
concerns alone where services are designed to maximise engagement. Guidance for families should therefore sit alongside wider action on persuasive design, age-appropriate defaults and platform accountability as outlined in Chapter 2.

#### **5.4 Parents want more support to use parental controls**

Parents would be better supported by parental controls that are standardised, easy to find, simple to set up, clearly explained, and enabled by default or prompted at key moments. The issue is not simply whether parents are willing to use controls, as many are. The challenge is that tools are spread across multiple parts of the digital ecosystem, use inconsistent naming conventions, and are not always easy to understand or apply consistently. Platforms should do more to explain what tools exist, what they do, and how parents can use them.

The current landscape is fragmented, with parents often needing to navigate different tools across devices, broadband and mobile networks, streaming services, apps and platforms, app stores, browsers and safety software. While 95% of parents tell us they are aware of at least one type of parental control or technical tool, this does not always translate into uptake and use (Figure 14). Awareness and use vary across different types of controls, pointing to a gap between awareness of tools and parents' ability to use them consistently in practice. For instance, 56% of parents are aware of broadband and mobile parental controls yet only 31% use them.<sup>154</sup>

**Figure 14. Parents’ awareness of parental controls and technical tools compared to usage**



**Figure 14. Parents’ awareness of parental controls and technical tools compared to usage** | Data from [Internet Matters Pulse](#) (November 2025).

This gap may be partly explained by the practical barriers parents face when setting up tools. 70% of parents say they have encountered a barrier when setting up parental controls, and the range of barriers experienced is wide. Barriers include having to set up new logins or accounts (23%), confusing or complicated steps (22%), the process taking too much time (19%), difficulty setting up controls across multiple devices (18%), being unsure what tools or settings to use (17%), and not being able to find clear instructions or guidance (17%).<sup>155</sup> These findings point to the need for parental controls to be simpler, more intuitive and easier to apply across the services and devices children use.

Greater standardisation would help parents use parental controls more effectively. *Internet Matters Pulse* finds that 83% of parents agree parental controls should be standardised across online platforms.<sup>156</sup> Government should work with industry to set stronger expectations for parental controls so they are more consistent in language, design and functionality, while still allowing parents to tailor settings to their child’s age, needs and maturity.

These findings show that parental controls need to be easier, clearer and more consistent. However, improving usability alone is not enough: protections also need to be enabled or prompted at the points when parents are most likely to need them.

### 5.5 Parental controls should be enabled by default and evolve with age

Parental controls should therefore be enabled by default or prompted to parents at key moments. This includes when a device is purchased or set up, when a child account is created, when a child downloads a new app or game, when a child reaches a new age threshold, and when platforms introduce new features.

*Internet Matters Pulse* suggests parents support stronger default protections: 39% support parental controls being automatically enabled on under-16s' social media accounts as an alternative to a blanket social media ban.<sup>157</sup>

This is particularly important at age-transition points. Protections should evolve with children's age and maturity, but they should not be switched off, weakened or presented to children as optional simply because a child reaches 13. *Internet Matters Pulse* finds that parents support default parental controls remaining in place beyond age 13: only 16% say parental controls should be on by default only up to age 13, while 36% say they should remain on by default up to age 16, 8% say up to age 17, and 17% say up to age 18. Just 2% say parental controls should not be on by default on children's accounts.<sup>158</sup> Recent media reporting about Google's Family Link has highlighted concerns about children being prompted directly to turn off parental controls when they approached 13, before Google changed its policy to require parental approval for under-18s to stop supervision.<sup>159</sup> Platforms should therefore design parental controls and child or teen accounts to evolve with age, rather than assuming that protections should fall away at 13.

Parents would also benefit from clear, simple explanations of what different controls do, what risks they help address, and what they do not cover. This should include age-based recommendations, simple in-product walkthroughs, reminders to review settings over time, and signposting to trusted independent guidance. Nearly half of parents (49%) say they are interested in information on how to set up and use parental controls, showing clear demand for practical support. Furthermore, two in five (38% of) parents who visit the Internet Matters website say they do so to get advice on how to set up parental controls.<sup>160</sup> Platforms should do more to engage parents directly, including through clear prompts, parent dashboards, accessible guidance and timely explanations when new tools or settings become available.

Internet Matters provides step-by-step parental control guides to help families layer controls across networks, devices, apps and platforms as children grow. Practical, independent guidance of this kind should be clearly signposted by services at key moments in the user journey, including device set-up, account creation and when children begin using new apps or platforms.

## 5.6 Support should be accessible to different families

Parental controls, screen time guidance and wider online safety advice should be designed for families with different levels of time, confidence, resources and digital literacy. It should not be assumed that all parents can confidently monitor, configure and troubleshoot settings across multiple services and devices. This reflects what parents tell us in our research: they recognise their own role, but also describe limits to what they can manage, including children bypassing controls, parents struggling to keep up with tools, and different rules applying across households.<sup>161</sup>

Internet Matters' *DWI Year 4* found that 20% of parents say they manage their children's online behaviour "a lot", but parents in higher socio-economic groups are more likely to do so than those in lower socio-economic groups (23% compared to 11%).<sup>162</sup> This suggests that parents' ability to actively manage children's online experiences may vary by confidence, time, resources or access to support.

Controls and guidance should also be flexible enough to reflect different children's needs. Some children, including children with additional needs or vulnerabilities, may need more tailored or sustained support. This should be reflected in how parental controls are designed, explained and reviewed over time, and in how screen time and online safety guidance is made available to families.

This reinforces the importance of the media and digital literacy support discussed in Chapter 4. Parents and carers need support that is practical, accessible and available in formats that reflect different levels of confidence, literacy, language, time and need.

## 5.7 Parental support must sit alongside platform responsibility

Even where parental controls are easier to use and better signposted, they cannot be the main line of defence. Parental controls, screen time guidance and media literacy support are only effective if they sit within a wider system of child safety. Parents should not be expected to compensate for services that are not designed with children's needs in mind, or for default settings that expose children to avoidable risk.

Services used by children should provide age-appropriate defaults, effective age assurance, clear reporting routes and restrictions on high-risk features where appropriate. Parental controls should give families additional ways to tailor children's experiences, rather than acting as the main line of defence.

This is particularly important because parents do not see online safety as solely their responsibility. Both parents and children see a role for Government, with 44% and 43% respectively saying Government could be doing more to keep children safe online.<sup>163</sup>

Government should therefore avoid framing parental controls, screen time guidance or media literacy support as substitutes for platform duties. Instead, these should form part of a wider package of protections, alongside safe-by-design services, age-appropriate defaults, effective regulation and clear accountability for industry.

## 5.8 What Government must do

Supporting families is not simply a matter of giving parents more responsibility. Parents and carers are already central to children's online safety, but they need tools that are easier to use, clearer to understand and better integrated across the services children access. They also need practical guidance, trusted information and support to have informed conversations with their children as they grow.

Government should therefore focus on:

- **Providing parents with more guidance, including on screen time.** This should include age-appropriate screen time guidance that helps families focus on balance, context and healthy habits.
- **Requiring parental controls to be easier, clearer and more consistent including through the introduction of more defaults and standardisation.** Government should set stronger expectations for parental controls across services, devices, app stores and platforms. Controls should be easy to find, simple to set up, clearly explained, consistent in language and design, enabled by default or prompted at key moments such as device set-up, account creation, app downloads and age transitions. They should also evolve with children's age and maturity, rather than assuming protections should fall away at 13, and allow parents to tailor settings to their child's age, maturity, development and needs.
- **Supporting parents as children grow.** Guidance and tools should reflect children's age, maturity, development and needs. Younger children may need stronger default protections, while older children may need more transparency, shared decision-making and support to build independence.
- **Making support accessible to different families.** Support should work for parents with different levels of digital confidence, time, literacy, language needs and access to technology. It should also include tailored support for parents of children with additional needs.
- **Signposting trusted independent advice.** Services, schools and Government should signpost parents to trusted resources, including practical guidance on parental controls, screen time, online harms and how to respond when a child needs help.
- **Ensuring parental support complements platform responsibility.** Parental controls, screen time guidance and media literacy support must not be treated as substitutes for safer design, effective age assurance, age-appropriate defaults and clear accountability for online services.

- **Communicating changes clearly to families.** Government should ensure that changes introduced following this consultation are accompanied by clear, practical guidance for parents, carers and children. This will be particularly important where changes affect how families experience online services in practice, such as new age checks or age-based restrictions. Families will need to understand what is changing, why it is happening, what role they are being asked to play, and where to go for trusted support.

A safer digital environment for children cannot depend on parents navigating a fragmented and complex set of tools alone. Families need better support, but online services must remain responsible for designing experiences that are safe and appropriate for children.

## References

---

- <sup>1</sup> House of Commons Library (2026), *Proposals to ban social media for children*. [Link](#).
- <sup>2</sup> Internet Matters (2026) *The Online Safety Act: Are children safer online?* [Link](#).
- <sup>3</sup> Internet Matters (2026) *Children's Wellbeing in a Digital World Year 5*. [Link](#).
- <sup>4</sup> Internet Matters (2025) *Children's Wellbeing in a Digital World Year 4*. [Link](#).
- <sup>5</sup> *Children's Wellbeing in a Digital World Year 5*. [Link](#).
- <sup>6</sup> Internet Matters (2025) *Informed or Overwhelmed?: Understanding the impact of online news on children and young people's wellbeing*. [Link](#).
- <sup>7</sup> *Children's Wellbeing in a Digital World Year 5*. [Link](#).
- <sup>8</sup> Internet Matters (2025) *Connected & Conflicted: Children's perspectives on restricting social media for under-16s*. [Link](#).
- <sup>9</sup> Ibid.
- <sup>10</sup> Ibid.
- <sup>11</sup> *Children's Wellbeing in a Digital World Year 5*. [Link](#).
- <sup>12</sup> Ibid.
- <sup>13</sup> Internet Matters (2025) *Me, Myself and AI: Understanding and safeguarding children's use of AI chatbots*. [Link](#).
- <sup>14</sup> Internet Matters (n.d.) *Internet Matters Pulse (November 2025)*. [Link](#).
- <sup>15</sup> *Internet Matters Pulse (November 2025)*. Unpublished.
- <sup>16</sup> *Internet Matters Pulse (November 2025)*. [Link](#).
- <sup>17</sup> Ibid.
- <sup>18</sup> Ibid.
- <sup>19</sup> *Children's Wellbeing in a Digital World Year 4*. [Link](#).
- <sup>20</sup> *Informed or Overwhelmed?* [Link](#).
- <sup>21</sup> Internet Matters (2026) *Preparing young voters in today's online information environment*. [Link](#).
- <sup>22</sup> *Internet Matters Pulse (November 2025)*. [Link](#).
- <sup>23</sup> *Me, Myself and AI*. [Link](#).
- <sup>24</sup> Internet Matters (2024) *More than a Game: Exploring neurodivergent young people's relationships with online games platforms*. [Link](#).
- <sup>25</sup> *Children's Wellbeing in a Digital World Year 5*. [Link](#).
- <sup>26</sup> Ibid.
- <sup>27</sup> Ibid.
- <sup>28</sup> eSafety Commissioner (2 April 2026) "Social media age restrictions". [Link](#).
- <sup>29</sup> ABC News (5 November 2025) "Which apps are included in Australia's social media ban?" [Link](#).
- <sup>30</sup> Internet Matters (n.d.) *Internet Matters Pulse (May 2026)*. Unpublished.
- <sup>31</sup> *The Online Safety Act: Are children safer online?* [Link](#).
- <sup>32</sup> *Internet Matters Pulse (May 2026)*. Unpublished.
- <sup>33</sup> *The Online Safety Act: Are children safer online?* [Link](#).
- <sup>34</sup> Internet Matters (2026) *The Gender Gap: Understanding and responding to girls' and boys' online experiences*. [Link](#).
- <sup>35</sup> *Children's Wellbeing in a Digital World Year 4*. [Link](#).
- <sup>36</sup> *More than a Game*. [Link](#).
- <sup>37</sup> *Preparing young voters in today's online information environment*. [Link](#).
- <sup>38</sup> *The Online Safety Act: Are children safer online?* [Link](#).
- <sup>39</sup> *Internet Matters Pulse (November 2025)*. [Link](#).
- <sup>40</sup> *Me, Myself and AI*. [Link](#).
- <sup>41</sup> *The Online Safety Act: Are children safer online?* [Link](#).

- 
- <sup>42</sup> Ibid.
- <sup>43</sup> *Internet Matters Pulse (May 2026)*. Unpublished.
- <sup>44</sup> Internet Matters (2023) *“It’s really easy to go down that path”*: Young people’s experiences of online misogyny and image-based abuse. [Link](#).
- <sup>45</sup> Internet Watch Foundation (2025) *Annual data and insights report 2025*. [Link](#).
- <sup>46</sup> NSPCC (September 2024) *“Young people’s experiences of online sexual extortion or ‘sextortion’”*. [Link](#).
- <sup>47</sup> Internet Watch Foundation (2025) *Annual data and insights report 2025*. [Link](#).
- <sup>48</sup> UNICEF (2026) *Artificial Intelligence and Child Sexual Abuse and Exploitation*. [Link](#).
- <sup>49</sup> *“It’s really easy to go down that path”*. [Link](#).
- <sup>50</sup> Ibid.
- <sup>51</sup> Ibid.
- <sup>52</sup> *Internet Matters Pulse (May 2026)*. Unpublished.
- <sup>53</sup> Internet Matters (18 December 2025) *“A year on: ‘Nudifying’ tools remain easy to access – and just as harmful”*. [Link](#).
- <sup>54</sup> NSPCC (N/A), *“Chat apps”*. [Link](#).
- <sup>55</sup> Ofcom (2025), *Register of Risks*. [Link](#).
- <sup>56</sup> *“It’s really easy to go down that path”*. [Link](#).
- <sup>57</sup> *Internet Matters Pulse (May 2026)*. Unpublished.
- <sup>58</sup> *Internet Matters Pulse (November 2025)*. [Link](#).
- <sup>59</sup> Internet Watch Foundation (2018) *Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse*. [Link](#).
- <sup>60</sup> *Internet Matters Pulse (November 2025)*. Unpublished.
- <sup>61</sup> UK Government (29 June 2021) *“Child online safety: Protecting children from online sexual exploitation and abuse”*. [Link](#).
- <sup>62</sup> Independent Inquiry Child Sexual Abuse (2020) *The Internet: Investigation Report*. [Link](#).
- <sup>63</sup> *Internet Matters Pulse (May 2026)*. Unpublished.
- <sup>64</sup> Ofcom (2024) *Protecting people from illegal harms online: Register of Risks*. [Link](#).
- <sup>65</sup> *Internet Matters Pulse (November 2025)*. [Link](#).
- <sup>66</sup> *Internet Matters Pulse (May 2026)*. Unpublished.
- <sup>67</sup> Internet Matters (2024) *“So standard it’s not noteworthy”*: Teenage girls’ experiences of harm online. [Link](#).
- <sup>68</sup> *Connected & Conflicted*. [Link](#).
- <sup>69</sup> Internet Matters (2024) *Digital Dilemmas: Parents’ perspectives on restricting children’s smartphone and social media use*. [Link](#).
- <sup>70</sup> eSafety Commissioner (10 December 2025) *“Location sharing.”* [Link](#).
- <sup>71</sup> *Internet Matters Pulse (May 2026)*. Unpublished.
- <sup>72</sup> *Children’s Wellbeing in a Digital World Year 5*. [Link](#).
- <sup>73</sup> GambleAware (2021) *Lifting the Lid on Loot-Boxes*. [Link](#).
- <sup>74</sup> House of Commons (2024) *Loot boxes in video games*. [Link](#).
- <sup>75</sup> Ofcom (2025) *Additional Safety Measures: Online Safety*. [Link](#).
- <sup>76</sup> *Internet Matters Pulse (May 2026)*. Unpublished.
- <sup>77</sup> *Internet Matters Pulse (November 2025)*. [Link](#).
- <sup>78</sup> *Children’s Wellbeing in a Digital World Year 5*. [Link](#).
- <sup>79</sup> Ibid.
- <sup>80</sup> Ibid.
- <sup>81</sup> *Connected & Conflicted*. [Link](#).
- <sup>82</sup> *The Online Safety Act: Are children safer online?* [Link](#).
- <sup>83</sup> Ibid.
- <sup>84</sup> Ibid.
- <sup>85</sup> Ibid.
- <sup>86</sup> *Connected & Conflicted*. [Link](#).
- <sup>87</sup> Ibid.

- 
- <sup>88</sup> *Informed or Overwhelmed?* [Link](#).
- <sup>89</sup> *Internet Matters Pulse (May 2026)*. Unpublished.
- <sup>90</sup> *Me, Myself and AI*. [Link](#).
- <sup>91</sup> *Ibid.*
- <sup>92</sup> *Ibid.*
- <sup>93</sup> *Internet Matters Pulse (May 2026)*. Unpublished.
- <sup>94</sup> *The Online Safety Act: Are children safer online?* [Link](#).
- <sup>95</sup> *Ibid.*
- <sup>96</sup> *Ibid.*
- <sup>97</sup> *Ibid.*
- <sup>98</sup> Internet Matters (4 December 2025) “New data shows no rise in children’s VPN use after the introduction of online age checks”. [Link](#).
- <sup>99</sup> National Cyber Security Centre (N/A) “Device security guidance”. [Link](#).
- <sup>100</sup> Internet Matters (11 April 2025) “Age assurance and online safety: What parents and children have to say”. [Link](#).
- <sup>101</sup> *Internet Matters Pulse (May 2026)*. Unpublished.
- <sup>102</sup> *Ibid.*
- <sup>103</sup> *Ibid.*
- <sup>104</sup> *Ibid.*
- <sup>105</sup> *Ibid.*
- <sup>106</sup> *Internet Matters Pulse (November 2025)*. Unpublished.
- <sup>107</sup> *Internet Matters Pulse (November 2025)*. [Link](#).
- <sup>108</sup> *Me, Myself and AI*. [Link](#).
- <sup>109</sup> *Ibid.*
- <sup>110</sup> *Informed or Overwhelmed?* [Link](#).
- <sup>111</sup> *Preparing young voters in today’s online information environment*. [Link](#).
- <sup>112</sup> *Ibid.*
- <sup>113</sup> *Internet Matters Pulse (November 2025)*. [Link](#).
- <sup>114</sup> *Children’s Wellbeing in a Digital World Year 5*. [Link](#).
- <sup>115</sup> *Internet Matters Pulse (November 2025)*. [Link](#).
- <sup>116</sup> “It’s really easy to go down that path”. [Link](#).
- <sup>117</sup> Internet Matters (2024) *Shifting the dial: Methods to prevent ‘self-generated’ child sexual abuse among 11-13-year-olds*. [Link](#).
- <sup>118</sup> *Connected & Conflicted*. [Link](#).
- <sup>119</sup> *Internet Matters Pulse (November 2025)*. [Link](#).
- <sup>120</sup> Internet Matters (2024) *A Vision for Media Literacy: Charting the path for media literacy in schools*. [Link](#).
- <sup>121</sup> *Informed or Overwhelmed?* [Link](#).
- <sup>122</sup> *Me, Myself and AI*. [Link](#).
- <sup>123</sup> UK Government (2025) *Curriculum and Assessment Review Final Report: government response*. [Link](#).
- <sup>124</sup> *Internet Matters Pulse (November 2025)*. [Link](#).
- <sup>125</sup> *Ibid.*
- <sup>126</sup> *Ibid.*
- <sup>127</sup> *Internet Matters Pulse (May 2026)*. Unpublished.
- <sup>128</sup> Internet Matters (2023) *Internet Matters data briefing: Online safety in schools*. [Link](#).
- <sup>129</sup> *Ibid.*
- <sup>130</sup> *Internet Matters Pulse (November 2025)*. Unpublished.
- <sup>131</sup> Internet Matters (2025) *Because children deserve a safe digital world: Impact Report 2024/25*. [Link](#).
- <sup>132</sup> BBFC (26 May 2026) “Parents twice as concerned about children’s online safety than their physical health”. [Link](#).
- <sup>133</sup> *Children’s Wellbeing in a Digital World Year 5*. [Link](#).

- 
- <sup>134</sup> *Children's Wellbeing in a Digital World Year 4*. [Link](#).
- <sup>135</sup> Ibid.
- <sup>136</sup> *More than a Game*. [Link](#).
- <sup>137</sup> *Children's Wellbeing in a Digital World Year 4*. [Link](#).
- <sup>138</sup> *Internet Matters Pulse (November 2025)*. Unpublished.
- <sup>139</sup> Ibid.
- <sup>140</sup> *More than a Game*. [Link](#).
- <sup>141</sup> *Me, Myself and AI*. [Link](#).
- <sup>142</sup> Ibid.
- <sup>143</sup> *Children's Wellbeing in a Digital World Year 5*. Unpublished data.
- <sup>144</sup> *Children's Wellbeing in a Digital World Year 4*. [Link](#).
- <sup>145</sup> UK Government, "Help your child stay safe online" (Accessed 12<sup>th</sup> May 2026). [Link](#).
- <sup>146</sup> *Internet Matters Pulse (November 2025)*. [Link](#).
- <sup>147</sup> *Digital Dilemmas*. [Link](#).
- <sup>148</sup> *Internet Matters Pulse (November 2025)*. [Link](#).
- <sup>149</sup> Ibid.
- <sup>150</sup> *Internet Matters Pulse (November 2025)*. Unpublished.
- <sup>151</sup> Ibid.
- <sup>152</sup> *Internet Matters Pulse (May 2026)*. Unpublished.
- <sup>153</sup> Ibid.
- <sup>154</sup> *Internet Matters Pulse (November 2025)*. [Link](#).
- <sup>155</sup> *Internet Matters Pulse (November 2025)*. Unpublished.
- <sup>156</sup> *Internet Matters Pulse (May 2026)*. Unpublished.
- <sup>157</sup> Ibid.
- <sup>158</sup> Ibid.
- <sup>159</sup> Mashable (13 January 2026) "Google reverses key parental control policy". [Link](#).
- <sup>160</sup> *Internet Matters Pulse (November 2025)*. Unpublished.
- <sup>161</sup> *The Online Safety Act: Are children safer online?* [Link](#).
- <sup>162</sup> *Children's Wellbeing in a Digital World Year 4*. [Link](#).
- <sup>163</sup> *Internet Matters Pulse (May 2026)*. Unpublished.