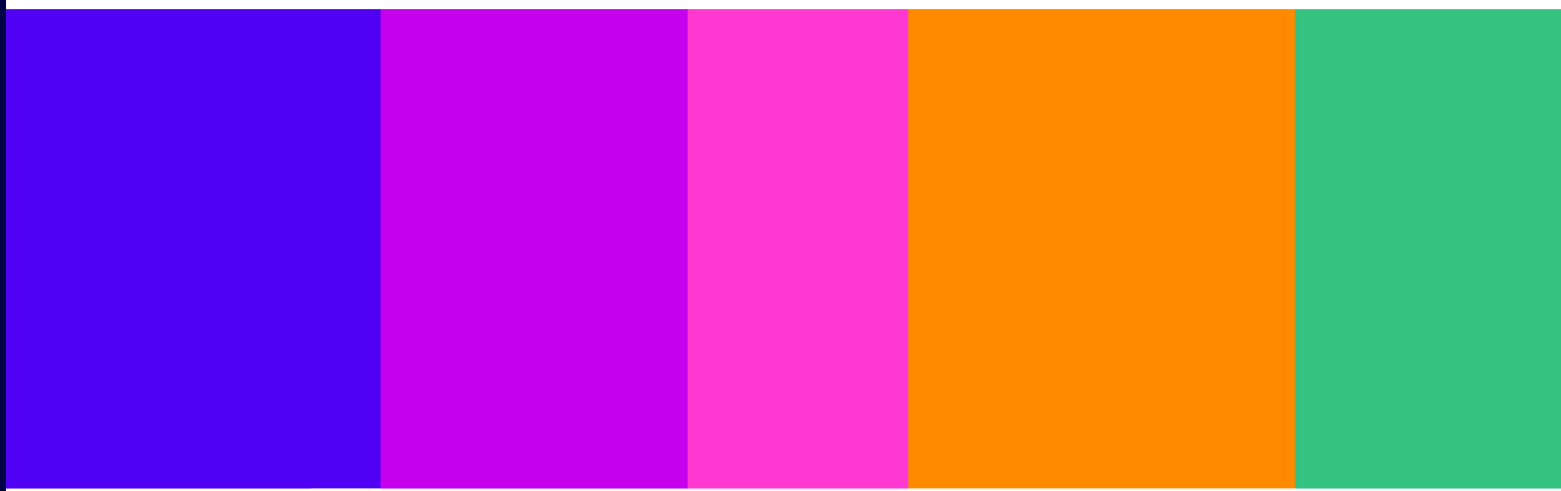


# Update: tech firms' responses to our call for action to protect children

---

**Report**

Published 21 May 2026



# Contents

---

## Section

Overview .....	3
What the services told us.....	6
Why we wrote to services in March .....	8
Summary of responses.....	11
Conclusion and next steps .....	14

## Annex

A1 Responses in full .....	16
----------------------------	----

# Overview

## Our challenge to the sites and apps most used by children

Duties on online services to protect children from harmful content came into effect in July 2025. Since then, we have seen much wider use of age assurance by tech firms to identify child users, and some important changes in the safety measures used to keep them safe.

However, our latest research into children's online experiences – carried out in November and December 2025, after the duties came into force – shows that much more needs to be done by tech firms to protect children. Seven in ten children aged 11-17 recall experiencing harmful content online – the same level reported in the research carried out in March and April 2025.<sup>1</sup> The services that are repeatedly mentioned by children as the sites where they are seeing this harmful content are the largest and most popular sites with children - not niche or specialist services. These findings mirror our and other organisations' research over many years. The historic lack of action by tech firms to tackle this is deeply concerning. Despite the national debate about the safety of children on these services, the lack of tangible improvements for children in our research suggests that, taken together, services have not to date made the scale of changes that are required.

On 12 March we wrote to the tech firms most popular with children – Facebook, Instagram, Roblox, Snapchat, TikTok and YouTube. We set out four areas where not enough is being done – our demands – and identified specific changes that each service could make to keep children in the UK safer online. Not all of our demands applied to all of the services. We required the services to be transparent about how they are protecting children and tell us what changes they'd make in light of these demands. We gave them seven weeks to respond.

Our demands were:

- **Failsafe grooming protections.** Ensure strict controls stop adults being able to contact children they do not know on their platforms. This includes using highly effective age assurance to check users' ages. The sexual exploitation and abuse of children online has devastating consequences for those affected. Online grooming crimes against children can include coercing a child to send sexual images of themselves, sexual extortion, and arranging in-person sexual abuse of a child.
- **Safer feeds for children.** Personalised content feeds are children's main pathway to harm online. Platforms must stop pushing harmful content to children in their feeds. This would reduce children's exposure to harmful content, including content promoting suicide, self-harm, and eating disorder content, ensuring platforms do not amplify risks through their design choices.
- **An end to product testing on children.** Companies must not test new products on children. They must conduct risk assessments for significant updates, such as the launch of new AI tools, to ensure these updates have been made safe for children before being deployed and tell Ofcom when they have done so. Children's safety must be considered before new features reach them. Safety by design is not optional. It is the law in the UK.
- **Effective minimum age policies.** Use highly effective age assurance to ensure children under the service's minimum age policy (often 13+) are not able to access the app or site. This

---

<sup>1</sup> Pg. 4, Children's Online Experiences Report, 2026, Ofcom

keeps younger children out of online spaces designed for older users, reducing their exposure to inappropriate content.

## Response to the challenge

In their responses to our demands, some firms have made significant new commitments to child safety. All of the services we wrote to have committed to going beyond what the Online Safety Act requires of them by notifying Ofcom when they update their risk assessments, except TikTok, which said it would notify us where required. This will mean that Ofcom can be made aware of new products and features before they are launched and made available to children. Ofcom can request these risk assessments and scrutinise the impact changes might have on children.

Snap committed to adopt all our grooming protection measures<sup>2</sup> by introducing default settings which ensure that stranger adults are not able to contact children, and children are not encouraged to expand their friendship groups to strangers. It has also committed to using highly effective age assurance to ensure these protections are available to all UK children. Snap has already begun testing this measure, using existing age signals. Snap has told us that over the summer it will ramp up work to rollout highly effective age assurance to all UK users to help to apply these grooming protections to under-18 Snapchat users in the UK. This is a necessary and important step, as Snap has been identified in a series of studies as a high-risk service for the grooming of UK children. We will monitor implementation closely to ensure effectiveness and completion by the end of the summer.

Meta committed to strengthening its anti-grooming protections by developing protections for children and by rolling out new AI tools to detect sexualised conversations with children. It is also extending “13+ movie style” sensitive content control, from Instagram to Facebook. It says this will make feeds safer by limiting the content teens see to a more age-appropriate level. These are potentially impactful changes. However, Meta has not committed to implement all our recommended anti-grooming measures, as set out in our Illegal Harms Codes of Practice, and we will continue to push it to adopt these, particularly our measure on network expansion prompts which we think is key to protecting children from strangers online.<sup>3</sup>

Roblox had previously made it harder for adults to contact children they do not know, turning off voice chat for U13s, and introducing highly effective age assurance to allow children to chat only with users in similar age groups, with the exception of trusted friends. It has now committed to go further, using highly effective age assurance to ensure only games suitable for the user’s age are suggested and giving parents the ability to switch off direct chat services entirely for U16s.

TikTok and YouTube have not committed to any significant changes in response to our specific demands. They maintain that their feeds are already safe for children. Of the three only Meta committed to new improvements to children’s feeds on Facebook, which will match existing levels of protection currently in place on Instagram.

Although they all acknowledge the importance of minimum age policies, we are not currently convinced that the commitments by any of the four services that set a strict minimum age of 13 in

---

<sup>2</sup> ‘All grooming measures’ refers to measures ICU F1 and ICU F2 in Ofcom’s Illegal Harms Codes of Practice as they currently apply today (and without prejudice to any updates Ofcom may make in the future).

<sup>3</sup> Service providers may seek to comply with a relevant duty in another way by adopting what the Act refers to as alternative measures. Where they take alternative measures, service providers must also maintain a record of what they have done and how they consider that it meets the relevant duties, including how they have complied with the duty to have particular regard to the importance of protecting freedom of expression and privacy.

their terms of use – Snapchat, Facebook, Instagram and TikTok – ensure they will effectively prevent children under 13 from accessing their sites and apps.

## Next steps

We welcome Snap’s commitment to action to prevent grooming. We expect its detailed roadmap for change by mid-June and will monitor implementation closely.

We welcome Meta’s commitments to strengthen its anti-grooming protections and to enhanced content controls and likewise we expect a detailed roadmap for change by mid-June. We will continue to press the company to adopt all our grooming prevention measures.

We welcome Roblox’s commitments to using highly effective age assurance to offer further chat protection to children. We will be scrutinising the rollout of its existing protections and monitoring the new commitments closely.

We are deeply concerned by the responses to the safer feeds demand. Our evidence published today shows that personalised feeds are the primary route through which children encounter harmful content.<sup>4</sup> It is particularly concerning that TikTok and YouTube have made no new commitments to make children’s feeds safer and appear to believe that their current approach is good enough.

We have used our information gathering powers to request detail from Meta, TikTok and YouTube, given the particularly high levels of usage of these services, on how they detect and prevent children being exposed to harmful content. We have received responses from all three services, which we are now scrutinising.

If our assessment concludes that services are not complying with their duties to use appropriate systems to prevent children’s exposure to harmful content, we will proceed to enforcement action. We will also consider scope to use new regulatory powers that require firms to undergo skilled persons’ reports and/or make their systems accessible for remote viewing. We will share our conclusions with government as it considers responses to its consultation ‘Growing up in the online world’, including potential new rules restricting children’s access to services that are built around personalised feeds.

Our research published today shows that nine in ten children aged 8-12 are using online services with a minimum age requirement of 13+,<sup>5</sup> so firms’ responses to our demand to enforce these requirements more effectively are concerning. We welcome the ICO’s ongoing work in this area and we will continue to work closely together. We have written to the Secretary of State for Science, Innovation and Technology to share our findings and to advise her that if the government wished to require tech firms to use highly effective age assurance to enforce their minimum age policies, this would need a clearer basis in legislation.

---

<sup>4</sup> Pg. 22, Children’s Online Experiences Report, Ofcom, 2026

<sup>5</sup> Pg. 10, Children’s Online Experiences Report, Ofcom, 2026

# What the services told us

## New commitments, but further action and disclosure needed

In the table below we set out the minimum necessary outcome for each of our demands, and which services we are most concerned about. The priority services are those where we expected to see new, explicit commitments to change, as we did not consider they were doing enough to protect children from harm.

Not all services were priorities for all our demands, for example because that service does not offer relevant functionality, or because its functionality poses a low risk.

The table is not an assessment of what impact the changes will have, as they have not yet been implemented. Rather it provides a snapshot illustrating the services' willingness to make changes to improve children's online safety following our challenge. In addition, this report is not an assessment of services' compliance with the Act. Where services fail to comply with their duties to protect children, we will take enforcement action where needed.<sup>6</sup>

Minimum necessary outcome	Priority services	Outcome status	What happens next?
<b>Protection from grooming</b> Children are protected from strangers contacting them.	Snapchat Facebook Instagram Roblox	Snap has committed to adopting all our grooming protection measures, backed up by use of Highly Effective Age Assurance.  Meta is developing a setting to manage teens' connection lists on Instagram.  Roblox has adopted significant grooming protections, and states these are supported by highly effective age assurance.	We will monitor Snap and Meta's implementation of their committed changes through regular progress updates and a detailed roadmap for change by mid-June.  We will continue to evaluate the impact Roblox's grooming protections are having on children's experiences.

<sup>6</sup> See further Ofcom's [Online Safety Enforcement Guidance](#) for details on when and how we enforce.

Minimum necessary outcome	Priority services	Outcome status	What happens next?
<b>Safer content feeds</b> Children are not exposed to harmful content on their feeds.	TikTok YouTube Facebook Instagram	Meta has committed to rolling out new content settings for under-18 Facebook users in the UK, which it claims will make children’s feeds safer. These settings are already in place on Instagram.  TikTok and YouTube have not committed to further changes.	We are interrogating responses to our legally binding information requests (RFIs) on recommender systems and content moderation. We are examining the scope to use novel powers (such as a skilled person report, remote viewing powers and testing).
<b>Transparency on risk</b> Ofcom is informed of emerging risks before new features launch, enabling timely oversight.	TikTok Roblox Snapchat YouTube Facebook Instagram	Meta, Roblox, Snap and YouTube have all committed to notify us when they have completed a significant change risk assessment.  TikTok said it would notify Ofcom when it updated its risk assessment due to a significant change, where required.	Evidence of shortcomings in risk management or safety outcomes would trigger regulatory intervention.
<b>Minimum age enforcement</b> Children are reliably prevented from accessing services below minimum age through highly effective age assurance.	Snapchat TikTok Facebook Instagram	Snap, TikTok and Meta have set out how they enforce their minimum age policies. We are not currently convinced these commitments ensure they’ll effectively prevent children under 13 from accessing their sites and apps.  The evidence shows many under 13s are continuing to access all these sites.	We have written to the Secretary of State advising why additional powers would be needed to enforce services’ age limits, and noting the link to the government’s live consultation ‘Growing up in the online world.’

We told services that they needed to reassure parents by publicly explaining how they are improving children’s safety. Only TikTok published a version of its response.<sup>7</sup> Others provided letters for Ofcom to publish on their behalf. Where non-confidential responses were provided, we have published them in full. We consider this reluctance to be fully transparent with parents and the public represents a missed opportunity for companies to have demonstrated how seriously they take children’s safety.

In the ‘Summary of responses’ section we provide more detail as to how the services responded to our demands.

---

<sup>7</sup>A link to the full blogpost can be found Annex 1

# Why we wrote to services in March

Rules to protect children from content that is harmful to them (the children’s safety duties) have now been in force for over nine months. After the laws came into force, we initially prioritised analysing services’ risk assessments to understand the risks of harm to children. We requested and received over one hundred risk assessments for analysis. Though some providers shared comprehensive and well-written records, we found unacceptable issues with many of the risk assessments we received. Through further engagement we received supplementary information or a revised risk assessment from services, with many amending risk levels as a result of our feedback. We took enforcement action against two providers for failure to respond to statutory information requests and carried out compliance remediation with Snap which resulted in it making significant changes to their risk ratings in a number of key areas.

Children’s safety is at the heart of our work. Our early enforcement has focused on the highest risk sites such as suicide forums and forums dedicated to harassment and abuse that have not engaged constructively or followed our rules. This has driven changes that will make children safer, such as highly risky file sharing services introducing hash-matching technology to detect child abuse material, or services that would not comply with their duties leaving the UK market. As a result of our engagement with the porn sector and associated enforcement action, age checks to restrict pornographic content to over-18s have been introduced by many of the most popular pornography sites in the UK. This includes the 10 most popular sites, which between them account for one quarter of all UK visitors to adult sites, all deploying age checks.

Despite these changes, when it comes to the largest sites – household names that children use the most – many have fallen short of putting children’s safety at the heart of their products. As our Children’s Online Experiences report published today demonstrates, Facebook, Instagram, Roblox, Snapchat, TikTok and YouTube continue to be some of the services most popular with children.<sup>8</sup> These platforms are also where children most frequently recall encountering harmful content.

Public trust in big tech firms is low, and the government is consulting on wider changes to protect children’s safety online. While some positive steps have been taken, it is clear that the limited progress does not reflect the urgency or scale of the risks children face. That is why we set out our demands, giving TikTok, Instagram, Facebook, YouTube, Snapchat and Roblox the opportunity to be transparent about how they are protecting children and highlighting the changes we think are needed.

## What the Children’s Online Experiences report tells us

A clear picture has been painted by our Children’s Online Experiences report published today. Not enough has changed to protect children from harm online between Wave 1 of our Children’s Online

---

<sup>8</sup> The children’s online experiences report summarises data and analysis on children’s online experiences before and shortly after the children’s safety duties became enforceable on 25 July 2025. The report does not cover the safety duties in the Act about illegal content. We determined the ‘most popular’ services by combining data on reach and time spent. Note also, Roblox was added at Wave 2 of our Children’s Online Safety Tracker, alongside Minecraft and Call of Duty to replace ‘Online games’, therefore no comparable data is available.

Safety Tracker (March - April 2025) and Wave 2 (November - December 2025), despite the children's safety duties becoming enforceable and our Protection of Children Codes of Practice ('Children's Codes') coming into effect in July 2025. Children still recalled seeing harmful content online across the largest online services.<sup>9</sup> Our research found:

- **At Wave 2, 84% of 8-12s said they had used one of the top five reaching online services (YouTube, Facebook, TikTok, Instagram and Snapchat) in a month, despite their minimum age requirement of 13+.**<sup>10</sup> Among children who recalled encountering harmful content online, TikTok was cited most often, followed by YouTube,<sup>11</sup> Instagram, Snapchat, Facebook, Roblox amongst other services.<sup>12</sup>
- **The services most popular with children has remained the same across the waves,** with YouTube reaching the most children, and Snapchat accounting for the most time out of an 8–14-year-old's day.<sup>13</sup> Among Snapchat users, children in the top quartile spent, on average, 4 hours 20 minutes per day on the service.
- **There was little change in overall exposure to harmful content for 11-17s.** Data from Wave 2 still shows around seven in ten (73%) 11-17-year-olds say they have seen or heard some form of harmful content online in a four-week period, comparable with Wave 1 data.
- **Personalised feeds remained the top route to content harmful to children at Wave 2.** When asked about one instance of exposure to harmful content, just over a third (35%) of 11-17-year-olds recalled exposure when they were 'scrolling on their feed'. 11-12-year-olds continued to face higher exposure to harmful content while playing an online game compared to older children.<sup>14</sup>
- **Content relating to bullying (62%) and hateful content (51%) remained the most common types of harmful content recalled by children at Wave 2,** with bullying showing a significant increase from Wave 1 (58%).

The research is clear. Online services have simply not yet done enough to make their services safe for children. Some of the largest services have not effectively implemented their own minimum age policies, meaning that children well below the minimum age are able to access these sites. The research also shows that children were still being exposed to harmful content after the children's safety duties came into force, and that personalised feeds remained the primary route through which this content was served to them.

---

<sup>9</sup> The term "harmful content" is used to refer collectively to primary priority content (PPC) and priority content (PC) only.

<sup>10</sup> The minimum age for Instagram, Facebook, Snapchat and TikTok is 13. The minimum age for Roblox is 5. Users must be at least 13 years old to use YouTube. Under 13s may use YouTube through a supervised account (with parental consent). This research is unable to establish the extent to which U13s were accessing YouTube via their own accounts or a supervised account.

<sup>11</sup> This data refers to YouTube specifically, not YouTube Kids for which exposure to harmful content was much lower.

<sup>12</sup> 25% of children aged 8-17 years recalled exposure to harmful content on WhatsApp, the same prevalence as Roblox.

<sup>13</sup> Identified through analysis of reach data, stated use and/or the time children spend on these services.

<sup>14</sup> At this point in the Children's Online Safety Tracker survey the sample were split via a 'least-fill quota' basis by type of content harmful to children encountered, to ensure that we maximised the potential sample size for each type of content harmful to children experienced. Additional weighting was then applied to the data to reflect the true proportion of type of content harmful to children encountered.

In addition to our own findings, research by the NSPCC found that online grooming offences have hit record levels across the UK. Figures published in November 2025 showed that 7,263 'Sexual Communication with a Child'<sup>15</sup> offences were recorded last year. The research also revealed that the services most commonly used by perpetrators to target children online (in cases where the platform could be identified) was led by Snapchat (40%), WhatsApp (9%), Facebook and Instagram (9%).<sup>16</sup>

---

<sup>15</sup> Offences under Section 15A of the Sexual Offences Act 2003.

<sup>16</sup> [Data shows how criminals are using private messaging platforms to manipulate and groom children | NSPCC](#)

# Summary of responses

## Snap

---

Snap sent us a confidential letter. It has not published its response.

In response to our four demands, Snap stated the following:

1. Snap committed to new improvements to reduce grooming on its service, signalling that it will switch off network expansion prompts for all child users by default and exclude child users from network expansion prompts for unknown users aged 18 or over by default, with the intended goal of preventing adult strangers from contacting children, as recommended by our Illegal Harms Codes of Practice. It has begun testing this measure now, using existing age signals. Over the summer, Snap will rollout highly effective age assurance to all UK users to ensure these grooming protections apply to all under-18 Snapchat users in the UK.
2. Snap did not comment on our safer feeds demand, but it was not a priority service for this demand area. Snap was not sent our recommender systems RFI.
3. Snap has committed to notify Ofcom when it has updated its risk assessment due to a significant change.
4. Our evidence shows that despite the minimum age requirement of 13, some under-13s may be accessing its service. Snap has committed to working at pace to implement HEAA and to working with the ICO and Ofcom to ensure progress on minimum age enforcement. We will continue to monitor any developments closely.

## Meta (Instagram and Facebook)

---

Meta sent us a confidential letter. It has not published its response.

In response to our four demands, Meta stated the following:

1. In relation to grooming, Meta has outlined plans to roll out AI tools to detect likely sexualised conversations between adults and teens in Instagram Direct messages to report offending accounts to NCMEC and take appropriate enforcement action. Meta is also developing a setting to manage teens' connection lists on Instagram.
2. In response to our safer feeds demand, Meta summarised its existing safety measures and outlined its plans to roll out stricter sensitive content settings for teens which are already available on Instagram, to Facebook. These new settings will show content appropriate for ages 13+, inspired by movie rating criteria and parent feedback. Meta also referenced improvements to its AI systems to improve the removal of harmful content and prevent it from being recommended.
3. Meta committed to notifying Ofcom when it has updated its risk assessment due to a significant change.
4. Meta shared some recently announced changes to help identify and remove under 13 accounts on Facebook and Instagram, including efforts to use enhanced AI technology as well as further future improvements.

## Roblox

---

Roblox provided a non-confidential response. We have published the non-confidential response below. It did not separately publish its response.

In response to our four demands, Roblox stated the following.

1. Roblox provided detail as to how existing measures help protect children from the risk of grooming. This includes recent changes placing children in bands based on age (backed by age assurance processes) so that they can only communicate with peers in similar age ranges with the exception of trusted friends. Roblox also confirmed it will be introducing two new age-based accounts for younger users in June 2026: Roblox Kids for users aged 5 to 8 and Roblox Select for users aged 9 to 15. All communications features within 'Roblox Kids' will be disabled by default, whilst chat is gradually introduced with safeguards within 'Roblox Select', with 9-12 year old accounts having different default communications settings to those aged 13-15.
2. Recommender systems on Roblox are used to suggest games and other gameplay items, not for an endless social-media-style feed. Due to this limited functionality, our safer feeds demand does not apply to Roblox, nor was it sent the RFI on recommender systems.
3. Roblox has said it will endeavour to notify us when there is a significant change leading to it updating its risk assessment.
4. Unlike the other services we wrote to, Roblox explained it actively encourages children under 13 to use its platform – its minimum age for use of the service is 5 years old. Roblox also set out its current process to determine user age and the age restrictions it applies to different age groups. It determines a user's age through a facial age check.

## YouTube

---

YouTube sent us a non-confidential letter. We have published the non-confidential response below. It did not separately publish this letter.

YouTube stated the following:

1. YouTube set out some of its current measures related to grooming, including restricted comment environments and proactive content safeguards for content including minors.
2. YouTube provided information related to its current protections in place for recommender systems. These include safeguards to reduce repeated recommendations of some content. It did not commit to any new measures.
3. YouTube committed to notifying Ofcom when it has updated its risk assessment due to a significant change.
4. YouTube provided information about its approach to age-appropriate access, including existing measures to protect children from harmful content, including YouTube Kids and voluntary Supervised Teens Accounts.

## TikTok

---

TikTok published a blog post which included a summary of the work it has done to remove accounts that belong to children under the age of 13 and the steps it has taken to protect children from

grooming. The blog covers a range of other safety topics and can be found in the Annex below.

TikTok also provided a confidential response to our four demands stating the following:

1. TikTok set out the measures it has taken to reduce the risk of grooming and limit contact from unknown adults.
2. TikTok explained how its recommender systems work and how existing measures protect children from harmful content feeds. It also confirmed it is engaging with our RFI relating to TikTok's recommender systems.
3. TikTok committed to engaging with Ofcom regarding changes to its platforms and said that it would, where required, notify Ofcom when it updated its risk assessment due to a significant change.
4. TikTok notes it is the only service to publish the number of suspected underage accounts it removes globally every quarter. TikTok also set out its current process to detect and remove children under 13 on its site.

# Conclusion and next steps

## Failsafe grooming protections

Snapchat committed to adopting all of our grooming measures. This includes, in broad terms, implementing our network expansion prompts measure and (backed up by highly effective age assurance) to stop strangers contacting children. This is a crucial step in children’s online safety given our research published today shows that children in the top quartile of Snapchat users aged 8–14 spend an average of 4 hours and 20 minutes per day on the service.<sup>17</sup>

Meta has also committed to adopting the connection list measure, though it has not yet agreed to implement the network expansion prompts safety measure within Ofcom’s Codes.

We welcome Roblox’s innovative approach to grooming protections, but these protections will only work robustly when backed up by highly effective age assurance.

Grooming can have devastating, lifelong consequences for children. We therefore welcome the commitments made by Snap, Meta and Roblox to strengthen protections. However, commitments must translate into action.

We will therefore be scrutinising the timeliness and effectiveness of how Snap, Meta and Roblox implement the changes they have committed to make. To support this, we have set clear deadlines for Snap and Meta by which we expect to see these changes in place. At the same time, we will continue to push Meta to adopt the network expansion prompts measure in full and expect to see a roadmap for improvements in the coming months. If the changes services have committed to are too slow or not properly implemented, we will not hesitate to act.

## Safer feeds for children

When harmful content is recommended to children, it is not by the choice of the child, it is by the design of the platform. Content feeds are a primary pathway to harm, and platforms must urgently fix this. We are therefore seriously concerned by the responses to the safer feeds demand. Overall, the responses failed to set out how the services will make feeds safe for children to use and reduce the harm that children experience.

Meta set out some planned changes, including new 13+ “movie-style” content settings currently available on Instagram that will be rolled out on Facebook. This is welcome, but it is too early to tell whether it will meaningfully reduce harm in practice. By contrast, YouTube and TikTok made no new commitments. Both restated existing measures and pointed to their responses to our RFIs. This is despite our research published today, which shows that TikTok and YouTube are the services most commonly recalled by children as sources of harmful content exposure, with just over a third saying they encountered such content while scrolling their feed.<sup>18</sup>

We are now scrutinising the detailed information request responses from Meta, YouTube and TikTok on how their recommender systems operate in practice and how they reduce risks to children. These are highly complex, largely automated systems. In order to independently verify what the services are telling us, we are examining the scope to use new regulatory powers, assigned to us by the Online Safety Act, such as requiring tech firms to undergo skilled persons’ reports and/or issuing remote viewing notices. Use of these powers would allow us to observe systems and processes in

---

<sup>17</sup> Pg. 4, Children’s Online Experiences Report, Ofcom, 2026

<sup>18</sup> Pg. 23, Children’s Online Experiences Report, Ofcom, 2026

real time; assess how platforms detect harmful content; how their age checks work and whether these measures are effective. We will assess whether use of these powers is necessary and proportionate, considering that independent scrutiny may be the only way of reaching a full and robust understanding of firms' systems, while acknowledging that such exercises can be resource-intensive and operationally complex.

Where services fail to comply with their duties to protect children, we will act and where needed, take enforcement action.

### Transparency on risk

There is already a legal duty to carry out risk assessments before implementing a significant change to their services. We asked them to commit to notifying us when they have completed these assessments. This goes beyond what is required by the Act but all services have confirmed they will do this (except TikTok, who said they would notify us where required). This demonstrates a serious commitment to online safety and shows willingness from services to go further than the Act requires.

However, while we welcome this commitment to increase transparency with us as the regulator, we are disappointed by the limited transparency to the public. Only TikTok published a public response to our demands. While some services provided us with non-confidential material, others shared information solely on a confidential basis. This was a missed opportunity for the services to improve transparency and strengthen public trust.

### Effective minimum age policies

While firms recognised the importance of minimum age policies, we are not currently convinced that the commitments by any of the four services that set a minimum age of 13 in their terms of use – Snapchat, Facebook, Instagram and TikTok – ensure they will effectively prevent children under 13 from accessing their sites and apps. Using highly effective age assurance to enforce minimum age policies is not currently a requirement of the Act. The evidence is clear that current processes are not good enough to stop access by under 13s – 84% of 8–12-year-olds are using these services.<sup>19</sup> Putting in place an effective age check to prevent underage users from setting up an account would make a significant difference to the safety of younger children.

Data protection law may provide a means of holding companies to account for effectively enforcing restrictions on under-13s' use, to prevent illegal processing of younger children's data. We welcome the work of the Information Commissioner's Office in this area. However, if the government and Parliament wished to directly require tech firms to enforce minimum age policies, this would need a clearer basis in online safety legislation.

We have written to the Secretary of State to set out this analysis, as the government considers responses to its 'Growing up in the online world' consultation.

---

<sup>19</sup> Children's Online Safety Tracker, Ofcom, 2026

# A1 Responses in full

Where services have published their responses, we have linked / attached the below in full.

Response from TikTok – Response was confidential, but blog post can be found [here](#).

[Response from Roblox](#)

[Response from YouTube](#)