Call for evidence response form

Please complete this form in full and return to os-cfe@ofcom.org.uk

Title
Second phase of online safety regulation: Protection of children

Full name
✂

Contact phone number
✂

Representing (select as appropriate)
[Please select]

Organisation name
Parent Zone

Email address
✂

Confidentiality

We ask for your contact details along with your response so that we can engage with you on this consultation. For further information about how Ofcom handles your personal information and your corresponding rights, see Ofcom's General Privacy Statement.

Your details: We will keep your contact number and email address confidential. Is there anything else you want to keep confidential? (select as appropriate)
[Please select]

Your response: Please indicate how much of your response you want to keep confidential (select as appropriate)
[Please select]

For confidential responses, can Ofcom publish a reference to the contents of your response? (select as appropriate)
[Please select]

Your response

Question 1: To assist us in categorising responses, please provide a description of your organisation, service or interest in protection of children online.
Is this a confidential response? (select as appropriate) *No*
Parent Zone sits at the heart of modern family life, providing advice, knowledge and support to shape the best possible future for children as they embrace the online world. We were founded in 2005 and since then have gone on to collaborate with many organisations who share our vision. The online world offers enormous opportunities to children, young people and families. We know it can also pose huge challenges. Our mission at Parent Zone is to improve outcomes in a connected world, so that children will be: • Safer online • Resilient to the challenges of the online world • Educated for a digital future

Question 2: Can you identify factors which might indicate that a service is likely to attract child users?
Is this a confidential response? (select as appropriate) *No*
There are numerous features designed explicitly to be attractive to children - bright colours, exciting narratives - but services should assume that children will go anywhere. Child users will access spaces that are not designed specifically for them, so provisions must be made regardless of whether or not a space is more or less 'likely' to attract children, as noted in the Californian Age Appropriate Design

Question 2: Can you identify factors which might indicate that a service is likely to attract child users?

Code (30/08/22)[1]: "Children should be afforded protections not only by online products and services specifically directed at them, but by all online products and services they are likely to access."

The online world should not be treated as distinct from the rest of life but as an extension of children's daily offline experience. In the offline, physical world, spaces exist that are designed specifically for children - play parks, soft play areas, schools - and, at the same time, children's needs are also accommodated in supermarkets and train stations and the multitude of other places that families visit.

We need to think beyond 'child-friendly' areas on the internet, and start from children's needs, and their rights of access. In some online spaces, supervised access will be appropriate, exactly as it is offline. Excluding children from the entirety of broader society online is likely to lead to workarounds and risk-taking behaviour.

We also need to be alert to the risks posed to young users of services that are supposedly targeted exclusively at adults. Design features that appeal to children are not simply visual but a matter of the way sites are structured. Our report, the Rip-off Games, found that games use gambling-like techniques to drive revenue in online games. Loot boxes function exactly like a lottery and employ psychological techniques developed by the gambling industry (such as variable rate reinforcement) to keep children playing and paying. Other forms of gambling use skins or other features from gaming as gambling chips on colourful fruit machines or games of chance. This is not a risk to a minority: 93% of children aged 8-16 regularly play online games[2].

Our sister site VoiceBox, run by young people for young people, has explored the attraction of in-stream payments to young people, now common on sites like Tik Tok[3] and Twitch, which tempt children with monetary rewards for activities they may undertake online. They have also looked at the nudge techniques used by mental health wellness apps[4] and found these target young people with mental health issues, reminding them of their unhappiness and keeping them seeking support.

---

[1] https://www.iwf.org.uk/report/?gclid=EAIaIQobChMI7t2A8p3i-QIVj4BQBh0W_Qr0EAAYASAAEgJZcfD_BwE
https://www.nytimes.com/2022/08/30/business/california-children-online-safety.html
[2] https://parentzone.org.uk/sites/default/files/2021-12/PZ_The_Rip-off_Games_2019.pdf
[3] https://voicebox.site/tiktok-live/
[4] https://voicebox.site/self-care-apps-monetisation/

Question 2: Can you identify factors which might indicate that a service is likely to attract child users?

We would argue that a better approach to the question of age is to ask which sites are not attractive to young people. The list would be much smaller.

Question 3: What information do services have about the age of users on different platforms (including children)?

Is this a confidential response? (select as appropriate)

[Please select]

Question 4: How can services ensure that children cannot access a service, or a part of it?

Is this a confidential response? (select as appropriate)

[Please select]

Question 5: What age assurance and age verification or related technologies are currently available to platforms to protect children from harmful content, and what is the impact and cost of using them?

Is this a confidential response? (select as appropriate)

[Please select]

Question 5: What age assurance and age verification or related technologies are currently available to platforms to protect children from harmful content, and what is the impact and cost of using them?

Question 6: Can you provide any evidence relating to the presence of content that is harmful to children on user-to-user and search services?

Is this a confidential response? (select as appropriate)

No

The coroner in Molly Rusell's inquest concluded that the content on the sites Molly Russell visited 'should not have been available for a 14-year-old child to see.' and this online content played a direct role in her death[5]. At the time, clearly, she was above the age at which it was considered acceptable for her to be on those platforms.

Pro-suicide and self-harm content should not be available to children, still less should they be bombarded by it by algorithms that detect an interest in it. We do, however, have concerns with the new regime's approach of classifying all under-18s as children: first, that it will incentivise over-monitoring by services; second, that children, seeing they are being over-protected, will seek to game the system and get around the restrictions.

The intention of the new regime is that children will be protected directly, by age assurance tools, and indirectly, by benefiting from a widespread use of tools to curate (make less harmful) adults' experience online - so that, for example, conspiracy theories should be less likely to take hold.

Again, we have a couple of reservations: first, as already mentioned, that this will lead to services miscategorising content, which in turn will result in a breakdown of trust in the system, including among children who will be incentivised into risk-taking. And, second, that the widespread reliance on algorithmic tools may end up being confusing and difficult for users. (Parents tell us they already struggle with

[5]https://www.judiciary.uk/wp-content/uploads/2022/10/Molly-Russell-Prevention-of-future-deaths-report-2022-0315_Published.pdf

Question 6: Can you provide any evidence relating to the presence of content that is harmful to children on user-to-user and search services?

the parental controls available to them.) We cannot expect by putting tools in place to absolve society at large of further responsibility, concern, or involvement.

The nature of the content that poses risks to young people is extremely broad, ranging from the illegal (grooming for child sexual exploitation) to slower-burn, more insidious kinds of content covered by the 'legal but harmful' designation in earlier iterations of the Online Safety Bill. This includes the normalisation of racism, as well documented by organisations like Kick it Out and Hope Not Hate. It also includes Violence Against Women and Girls as surfaced by organisations such as Glitch'; and disinformation, as monitored by Full Fact. All of these organisations have appeared on the Parent Zone podcast, Tech Shock[6].

In conversations with parents and local authorities through our media literacy programme, Parent Zone Local[7], a range of parental concerns were raised around the content to which their children are exposed, including:

- the lack of capacity to oversee children's online lives
- addictive design
- grooming
- radicalisation
- online gaming

We also hear concern from young people and parents about the toxic environments children are expected to tolerate in digital environments, including gaming. Not all of this toxicity is user-generated and we have concerns that consequently it will not be in scope of the new regime. Research carried out by Parent Zone and Ipsos MORI[8] found that almost half (49%) of children who play video games believe that they are only fun when you spend money. While they are gaming, children are exposed to endless psychological techniques designed to induce spending.

Content designed to groom young people into risk-taking behaviours can be seen in the attitudes of teenage girls towards Only Fans, as recorded by VoiceBox's research, which noted that 'creators speak about online pimps, disguised as 'promoters' and 'managers', who actively prey upon young girls on various social media platforms to encourage them to produce content on OnlyFans'. Even with an 18+ rating, we heard anecdotal evidence of grooming of children, encouraging them

---

[6] https://parentzone.org.uk/article/tech-shock-podcast-sanjay-bhandari
[7] The early stages of the PZ Local project involved three co-design sessions with key stakeholders: our local authority partners and parents, Jan 2023.
[8] https://parentzone.org.uk/sites/default/files/2021-12/PZ_The_Rip-off_Games_2019.pdf

Question 6: Can you provide any evidence relating to the presence of content that is harmful to children on user-to-user and search services?

to participate as soon as they are able.[9] This grooming often occurs on other platforms such as Twitter highlighting a wider ecosystem of harm that creates environments that foster risk.

Question 7: Can you provide any evidence relating to the impact on children from accessing content that is harmful to them?

Is this a confidential response? (select as appropriate)

[Please select]

Question 8: How do services currently assess the risk of harm to children in the UK from content that is harmful to them?

Is this a confidential response? (select as appropriate)

[Please select]

Question 9: What are the exacerbating risk factors services do or should consider which may have an impact on the risk of harm to children in the UK?

Is this a confidential response? (select as appropriate)

[Please select]

---

[9] https://voicebox.site/assets/onlyfansreport.pdf

Question 9: What are the exacerbating risk factors services do or should consider which may have an impact on the risk of harm to children in the UK?

Question 10: What are the governance, accountability and decision-making structures for child user and platform safety?

Is this a confidential response? (select as appropriate)

[Please select]

Question 11: What can providers of online services do to enhance the clarity and accessibility of terms of service and public policy statements for children (including children of different ages)?

Is this a confidential response? (select as appropriate)

No

Online services can use clear language that is accessible to children. This can include adding definitions to terms that may be unclear to younger users, and addressing the user directly. Good practice of this can be seen with the terms and conditions for the app Ollee[10], developed by Parent Zone with funding from Children in Need.

Terms of service that aim to protect children must also be accessible to, and read by parents. During our work with parents through programmes such as Parent Zone Local, we have been able to see firsthand the lack of understanding parents have in

---

[10] https://app.ollee.org.uk/#/privacy-and-terms

Question 11: What can providers of online services do to enhance the clarity and accessibility of terms of service and public policy statements for children (including children of different ages)?

these areas. Even the most digitally engaged parent can be defeated by terms of service that extend to several pages of dense legalese. We would like to several steps taken to improve and enhance clarity including:

- A radically simplified approach based on food labelling that gives an indication of risk through a simple rating.
- A national approach to age-rating sites that gives parents proper information in order to make informed decisions.
- A standardised 'pattern library' for terms of service that includes - for example - standard ways to present the 'manage cookies' option.
- A requirement for all terms of service to be available in multiple formats.

Question 12: How do terms of service or public policy statements treat 'primary priority' and 'priority' harmful content?[11]

Is this a confidential response? (select as appropriate)

[Please select]

Question 13: What can providers of online services do to enhance children's accessibility and awareness of reporting and complaints mechanisms?

Is this a confidential response? (select as appropriate)

No

---

[11] See A1.2 to A1.3 of the call for evidence for more information on the indicative list of harms to children.

Question 13: What can providers of online services do to enhance children's accessibility and awareness of reporting and complaints mechanisms?

Parent Zone welcomes provisions in the bill designed to ensure that users can easily navigate complaints procedures. But these provisions offer little comfort to parents, who feel there is a distinct lack of options for them to intervene on behalf of their children.

 Children should not be expected to bear the responsibility for taking on complex reporting systems without aid; it is imperative that parents be able to act on their behalf.

Parents want to be involved in their children's online lives, most especially when their children experience harm. They should have access to a proper parental complaints procedure. Parent Zone routinely provides support to parents who are frustrated by the lack of options available to them, demonstrating the need for specialised support. There are specialised reporting systems for child sexual abuse online through the IWF; for teachers facing abuse; and for young people. One is also needed for adults with parenting responsibility. It is essential that parents can access help when they become aware that their child is experiencing harm online.

Question 14: Can you provide any evidence or information about the best practices for accurate reporting and/or complaints mechanisms in place for legal content that is harmful to children, or users who post this content, and how these processes are designed and maintained?

Is this a confidential response? (select as appropriate)

[Please select]

Question 15: What actions do or should services take in response to reports or complaints about online content harmful to children (including complaints from children)?

Is this a confidential response? (select as appropriate)

No

When services respond to reports or complaints about online content harmful to children, speed is of the essence. Ofcom should provide guidance to services regarding the optimum length of time within which they should reply to reports and complaints, and these should be incorporated into platforms' reports and complaints processes.

Crucially, parents should be included in the processes, particularly where children are unable to fully articulate their grievances by themselves. If disputes become impossible to resolve and eventually require attention from Ofcom, this could be handled by a super complainant intermediary or ombudsman.

We also believe that services' responsibility doesn't end with a decision regarding reports and complaints, but should incorporate the recovery of the child concerned. Platforms have a duty to prevent children being exposed to online harm and, where they fail, they have a responsibility to help rebuild confidence online. The UKCIS Digital Resilience Framework[12]outlines how such support is key to recovery: services should not require the user to do all the work.

Putting the onus on parents to navigate the reporting process without support and backup makes it much harder for children to build digital resilience in the long-term. The Framework outlines tools and approaches that companies could introduce to support parents and focus effort on a child's recovery.

Question 16: What functionalities or features currently exist that are designed to prevent or mitigate the risk or impact of content that is harmful to children? A1.21 in the call for evidence provides some examples of functionalities.

Is this a confidential response? (select as appropriate)

[Please select]

---

[12]Digital Resilience Framework - GOV.UK

Question 16: What functionalities or features currently exist that are designed to prevent or mitigate the risk or impact of content that is harmful to children? A1.21 in the call for evidence provides some examples of functionalities.

Question 17: To what extent does or can a service adopt functionalities or features, designed to mitigate the risk or impact of content that is harmful to children on that service?

Is this a confidential response? (select as appropriate)

[Please select]

Question 18: How can services support the safety and wellbeing of UK child users as regards to content that is harmful to them?

Is this a confidential response? (select as appropriate)

No

First and foremost, services can support the safety and wellbeing of UK child users by ensuring that children are not exposed to harmful content. This doesn't mean simply excluding them from online activities, with blanket bans that will negatively impact children's rights. It means taking a safeguarding approach, so that when platforms become aware that a child is at risk of exposure to harm, they will act to prevent it. In other words, it's not about blocking off absolutely everything upstream, but taking a more downstream approach, based on what platforms know of a child's age and what they observe of behaviour patterns (as they knowingly did not do in the case of Molly Russell.)

Question 18: How can services support the safety and wellbeing of UK child users as regards to content that is harmful to them?

Parents understand the importance of media literacy for children in protecting their children from harm online. Our research with Meta[13] has shown for example that many parents adopt a 'pinch of salt' approach over disinformation, telling their children not to believe everything they see online. Furthermore, 12% of parents seek to enhance their media literacy, and they shared the steps taken with us:

- actively supporting children – having discussions as a family.
- doing research – finding multiple sources, using trusted/reputable sources, seeing what others say about the reliability of a site.
- having safe-lists of approved/trusted channels and sites.

Parents and children should be supported by funding and practical projects in their efforts to develop their children's media literacy, and their own, and to encourage digital resilience, giving children the ability to recognise and manage risk.

Question 19: With reference to content that is harmful to children, how can a service mitigate any risks to children posed by the design of algorithms that support the function of the service (e.g. search engines, or social and content recommender systems)?

Is this a confidential response? (select as appropriate)

[Please select]

Question 20: Could improvements be made to content moderation to deliver greater protection for children, without unduly restricting user activity? If so, what?

Is this a confidential response? (select as appropriate)

[Please select]

---

[13] https://parentzone.org.uk/sites/default/files/2023-02/Your%20Digital%20Family%20-%20The%20Listening%20Project%20guide.pdf

Question 20: Could improvements be made to content moderation to deliver greater protection for children, without unduly restricting user activity? If so, what?

Question 21: What automated, or partially automated, moderation systems are currently available (or in development) for content that is harmful to children?

Is this a confidential response? (select as appropriate)

[Please select]

Question 22: How are human moderators used to identify and assess content that is harmful to children?

Is this a confidential response? (select as appropriate)

[Please select]

Question 23: What training and support is or should be provided to moderators?

Is this a confidential response? (select as appropriate)

[Please select]

Question 23: What training and support is or should be provided to moderators?

Question 24: How do human moderators and automated systems work together, and what is their relative scale? How should services guard against automation bias?

Is this a confidential response? (select as appropriate)

[Please select]

Question 25: In what instances is content that is harmful to children, that is in contravention of terms and conditions, removed from a service or the part of a service that children can access?

Is this a confidential response? (select as appropriate)

[Please select]

Question 26: What other mitigations do services currently have to protect children from harmful content?

Is this a confidential response? (select as appropriate)

No

Question 26: What other mitigations do services currently have to protect children from harmful content?

There are already many tools available online. Our research found that platforms[14] have an average of 15 tools for parents to use, taking an average of 80 minutes to activate. Parents tell us, however, that they find these tools hard to locate and difficult to use. When they use them to complain, they feel their complaints disappear into the ether, when what they want is a prompt response.

We are concerned that the Bill's emphasis on tools to protect users from toxic content will lead to the release of a plethora of tools (leaving the underlying problems of toxicity not dealt with). There is a danger that parents will be bewildered and confused. They are often not on the same platforms as their children.

It is imperative that standards are set for any optional tools designed to protect both children and adults, and that these include visibility and ease of use.

Tools have a role to play; but they can be used as a fig leaf by platforms who can point to them as evidence that they are 'doing something'. Ofcom will need to be satisfied that they really are doing something, meaning that they are in widespread use.

Meanwhile, tools are not a substitute for safer design or for media literacy that enables users to understand how and why they are seeing what they see. Platforms and services should take their share of responsibility for all aspects of online safety - including safer design such as not privileging toxic content; and for media literacy. They should not assume that they can simply bolt on a bundle of tools and be done with it.

Question 27: Where children attempt to circumvent mitigations in place on a service, what further systems and processes can a service put in place to protect children?

Is this a confidential response? (select as appropriate)

[Please select]

---

[14] We investigated the number of tools and the time it takes to apply them across a number of platforms: Google Search Engine, Facebook, Instagram, TikTok, Snapchat, Youtube, Youtube Kids and Whatsapp (March 2023)

Question 27: Where children attempt to circumvent mitigations in place on a service, what further systems and processes can a service put in place to protect children?

Question 28: Other than those covered above in this document (the call for evidence), are you aware of other measures available for mitigating the risk, and impact of, harm from content that is harmful to children?

Is this a confidential response? (select as appropriate)

[Please select]