Consultation response form

Please complete this form in full and return to protectingchildren@ofcom.org.uk.

Consultation title	Consultation: Protecting children from harms online
Organisation name	Qoria Limited, Smoothwall

Your response

Question	Your response
Volume 2: Identifying the services children are using **Children's Access Assessments (Section 4).**	
Do you agree with our proposals in relation to children's access assessments, in particular the aspects below. Please provide evidence to support your view. 1. Our proposal that service providers should only conclude that children are not normally able to access a service where they are using highly effective age assurance? 2. Our proposed approach to the child user condition, including our proposed interpretation of "significant number of users who are children" and the factors that service providers consider in assessing whether the child user condition is met? 3. Our proposed approach to the process for children's access assessments?	We believe standards for age-appropriate content and services should be developed and online platforms should use APIs to allow on-device safety technology to direct users to the age-appropriate versions of the online platforms. This operates very well with YouTube, Google and Edge Search today. Parental controls and school safety apps can intercept requests to go to YouTube, Google/Edge Search and force a user to a maturity appropriate version (eg hiding adult content, comments or previews). Age assurance or verification is unnecessary to support this policy objective. Proposals to use age-verification gates to keep children safe make a number of unlikely or erroneous assumptions. Firstly, such a regime can only focus on a small number of online platforms. The reality is that toxicity and misbehaviour occurs vastly beyond the mainstream porn and social platforms. Secondly, teenagers will find it trivial to bypass age-verification through either VPNs or the increasing number of bio-hacks which are developing with the AI revolution. Thirdly, young children access adult content through many means other than the major porn sites. Age verification does not deal with search previews, message sharing, content shared in social & gaming platforms or inadvertent access through shared & parent devices (which will have verification tokens on them). And lastly, we believe it is ambitious to believe community support will be there for a measure which not only impacts significantly more adults than have children but will also drive concerns around privacy and tracking. The only truly reliable and effective approach to controlling a child's online activity is by controlling the device they're using.

Question	Your response
	On-device safety technology is available today, is trustworthy and proven on 10s of millions of devices. However, this technology is being deliberately limited by Google, Apple and Microsoft on their own devices and compromised for 3rd party parental controls. It is not however compromised when offered to app developers (like us) to build solutions for businesses and big schools. Note, this anti-competitive and harmful behaviour has been evidenced by competition inquiries in the EU, US and Australia. When installed by enterprises, on-device safety tech can deliver all of the core needs of the UK community. Porn blocking, social media age restrictions, screentime management, visibility and alerting, are easy to use and extremely difficult to bypass. What the UK urgently needs is regulations which ensure parents have the same access to the safety technology that big enterprises enjoy. With this, there will be a fundamental upgrade of safety capability available for UK parents and schools and market forces will then ensure emerging needs are catered for. We urge OFCOM to recommend an inquiry into methods to ensure competitive and open markets for on-device technology.
Volume 3: The causes and impacts of online harm to children **Draft Children’s Register of Risk (Section 7)**	
Proposed approach: 4. Do you have any views on Ofcom’s assessment of the causes and impacts of online harms? Please provide evidence to support your answer. a. Do you think we have missed anything important in our analysis? 5. Do you have any views about our interpretation of the links between risk factors and different kinds of content harmful to children? Please provide evidence to support your answer.	As discussed above, we can demonstrate that age assurance or verification is unnecessary to support this policy objective. Proposals to use age-verification gates to keep children safe make a number of unlikely or erroneous assumptions. Firstly, such a regime can only focus on a small number of online platforms. The reality is that toxicity and misbehaviour occurs vastly beyond the mainstream porn and social platforms. Secondly, teenagers will find it trivial to bypass age-verification through either VPNs or the increasing number of bio-hacks which are developing with the AI revolution. Thirdly, young children access adult

Question	Your response
6. Do you have any views on the age groups we recommended for assessing risk by age? Please provide evidence to support your answer. 7. Do you have any views on our interpretation of non-designated content or our approach to identifying non-designated content? Please provide evidence to support your answer. **Evidence gathering for future work:** 8. Do you have any evidence relating to kinds of content that increase the risk of harm from Primary Priority, Priority or Non-designated Content, when viewed in combination (to be considered as part of cumulative harm)? 9. Have you identified risks to children from GenAI content or applications on U2U or Search services? a) Please Provide any information about any risks identified 10. Do you have any specific evidence relevant to our assessment of body image content and depressive content as kinds of non-designated content? Specifically, we are interested in: a) (i) specific examples of body image or depressive content linked to significant harms to children, b. (ii) evidence distinguishing body image or depressive content from existing categories of priority or primary priority content. 11. Do you propose any other category of content that could meet the definition of NDC under the Act at this stage? Please provide evidence to support your answer.	content through many means other than the major porn sites. Age verification does not deal with search previews, message sharing, content shared in social & gaming platforms or inadvertent access through shared & parent devices (which will have verification tokens on them). And lastly, we believe it is ambitious to believe community support will be there for a measure which not only impacts significantly more adults than have children but will also drive concerns around privacy and tracking. The only truly reliable and effective approach to controlling a child's online activity is by controlling the device they're using. On-device safety technology is available today, is trustworthy and proven on 10s of millions of devices. However, this technology is being deliberately limited by Google, Apple and Microsoft on their own devices and compromised for 3rd party parental controls. It is not however compromised when offered to app developers (like us) to build solutions for businesses and big schools. Note, this anti-competitive and harmful behaviour has been evidenced by competition inquiries in the EU, US and Australia. When installed by enterprises, on-device safety tech can deliver all of the core needs of the UK community. Porn blocking, social media age restrictions, screentime management, visibility and alerting, are easy to use and extremely difficult to bypass. What the UK urgently needs is regulations which ensure parents have the same access to the safety technology that big enterprises enjoy. With this, there will be a fundamental upgrade of safety capability available for UK parents and schools and market forces will then ensure emerging needs are catered for. We urge OFCOM to recommend an inquiry into methods to ensure competitive and open markets for on-device technology.

Question	Your response
Draft Guidance on Content Harmful to Children (Section 8)	
12. Do you agree with our proposed approach, including the level of specificity of examples given and the proposal to include contextual information for services to consider? 13. Do you have further evidence that can support the guidance provided on different kinds of content harmful to children? 14. For each of the harms discussed, are there additional categories of content that Ofcom a) should consider to be harmful or b) consider not to be harmful or c) where our current proposals should be reconsidered?	No additional comments.
Volume 4: How should services assess the risk of online harms? **Governance and Accountability (Section 11)**	
15. Do you agree with the proposed governance measures to be included in the Children's Safety Codes? a) Please confirm which proposed measure your views relate to and explain your views and provide any arguments and supporting evidence. b) If you responded to our Illegal Harms Consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response. 16. Do you agree with our assumption that the proposed governance measures for Children's Safety Codes could be implemented through the	As discussed above, we can demonstrate that age assurance or verification is unnecessary to support this policy objective. Proposals to use age-verification gates to keep children safe make a number of unlikely or erroneous assumptions. Firstly, such a regime can only focus on a small number of online platforms. The reality is that toxicity and misbehaviour occurs vastly beyond the mainstream porn and social platforms. Secondly, teenagers will find it trivial to bypass age-verification through either VPNs or the increasing number of bio-hacks which are developing with the AI revolution. Thirdly, young children access adult content through many means other than the major porn sites. Age verification does not deal with search previews, message sharing, content shared in social & gaming platforms or inadvertent access through shared & parent devices (which will have verification tokens on

Question	Your response
same process as the equivalent draft Illegal Content Codes?	them). And lastly, we believe it is ambitious to believe community support will be there for a measure which not only impacts significantly more adults than have children but will also drive concerns around privacy and tracking. The only truly reliable and effective approach to controlling a child's online activity is by controlling the device they're using. On-device safety technology is available today, is trustworthy and proven on 10s of millions of devices. However, this technology is being deliberately limited by Google, Apple and Microsoft on their own devices and compromised for 3rd party parental controls. It is not however compromised when offered to app developers (like us) to build solutions for businesses and big schools. Note, this anti-competitive and harmful behaviour has been evidenced by competition inquiries in the EU, US and Australia. When installed by enterprises, on-device safety tech can deliver all of the core needs of the UK community. Porn blocking, social media age restrictions, screentime management, visibility and alerting, are easy to use and extremely difficult to bypass. What the UK urgently needs is regulations which ensure parents have the same access to the safety technology that big enterprises enjoy. With this, there will be a fundamental upgrade of safety capability available for UK parents and schools and market forces will then ensure emerging needs are catered for. We urge OFCOM to recommend an inquiry into methods to ensure competitive and open markets for on-device technology.
Children's Risk Assessment Guidance and Children's Risk Profiles' (Section 12)	
17. What do you think about our proposals in relation to the Children's Risk Assessment Guidance? a) Please provide underlying arguments and evidence of efficacy or risks that support your view.	No additional comment.

Question	Your response
18. What do you think about our proposals in relation to the Children's Risk Profiles for Content Harmful to Children? a) Please provide underlying arguments and evidence of efficacy or risks that support your view. Specifically, we welcome evidence from regulated services on the following: 19. Do you think the four-step risk assessment process and the Children's Risk Profiles are useful models to help services understand the risks that their services pose to children and comply with their child risk assessment obligations under the Act? 20. Are there any specific aspects of the children's risk assessment duties that you consider need additional guidance beyond what we have proposed in our draft? 21. Are the Children's Risk Profiles sufficiently clear and do you think the information provided on risk factors will help you understand the risks on your service? a) If you have comments or input related to the links between different kinds of content harmful to children and risk factors, please refer to Volume 3: Causes and Impacts of Harms to Children Online which includes the draft Children's Register of Risks.	
Volume 5 – What should services do to mitigate the risk of online harms **Our proposals for the Children's Safety Codes (Section 13)**	

Question	Your response
Proposed measures 22. Do you agree with our proposed package of measures for the first Children's Safety Codes? a) If not, please explain why. **Evidence gathering for future work.** 23. Do you currently employ measures or have additional evidence in the areas we have set out for future consideration? a) If so, please provide evidence of the impact, effectiveness and cost of such measures, including any results from trialling or testing of measures. 24. Are there other areas in which we should consider potential future measures for the Children's Safety Codes? a) If so, please explain why and provide supporting evidence.	No. As discussed above, we believe standards for age appropriate content and services should be developed and online platforms should use APIs to allow on-device safety technology to direct users to the age-appropriate versions of the online platforms. This operates very well with YouTube, Google and Edge Search today. Parental controls and school safety apps can intercept requests to go to YouTube, Google/Edge Search and force a user to a maturity appropriate version (eg hiding adult content, comments or previews). Age assurance or verification is unnecessary to support this policy objective. Proposals to use age-verification gates to keep children safe make a number of unlikely or erroneous assumptions. Firstly, such a regime can only focus on a small number of online platforms. The reality is that toxicity and misbehaviour occurs vastly beyond the mainstream porn and social platforms. Secondly, teenagers will find it trivial to bypass age-verification through either VPNs or the increasing number of bio-hacks which are developing with the AI revolution. Thirdly, young children access adult content through many means other than the major porn sites. Age verification does not deal with search previews, message sharing, content shared in social & gaming platforms or inadvertent access through shared & parent devices (which will have verification tokens on them). And lastly, we believe it is ambitious to believe community support will be there for a measure which not only impacts significantly more adults than have children but will also drive concerns around privacy and tracking. The only truly reliable and effective approach to controlling a child's online activity is by controlling the device they're using. On-device safety technology is available today, is trustworthy and proven on 10s of millions of devices. However, this technology is being deliberately limited by Google, Apple and Microsoft on their own devices and compromised for 3rd party parental controls. It is not

Question	Your response
	however compromised when offered to app developers (like us) to build solutions for businesses and big schools. Note, this anti-competitive and harmful behaviour has been evidenced by competition inquiries in the EU, US and Australia. When installed by enterprises, on-device safety tech can deliver all of the core needs of the UK community. Porn blocking, social media age restrictions, screentime management, visibility and alerting, are easy to use and extremely difficult to bypass. What the UK urgently needs is regulations which ensure parents have the same access to the safety technology that big enterprises enjoy. With this, there will be a fundamental upgrade of safety capability available for UK parents and schools and market forces will then ensure emerging needs are catered for. We urge OFCOM to recommend an inquiry into methods to ensure competitive and open markets for on-device technology.

Developing the Children’s Safety Codes: Our framework (Section 14)	
25. Do you agree with our approach to developing the proposed measures for the Children’s Safety Codes? a) If not, please explain why. 26. Do you agree with our approach and proposed changes to the draft Illegal Content Codes to further protect children and accommodate for potential synergies in how systems and processes manage both content harmful to children and illegal content? a) Please explain your views. 27. Do you agree that most measures should apply to services that are either large services or smaller services that present a medium or high level of risk to children? 28. Do you agree with our definition of ‘large’ and with how we apply this in our recommendations? 29. Do you agree with our definition of ‘multi-risk’ and with how we apply this in our recommendations? 30. Do you agree with the proposed measures that we recommend for all services, even those that are small and low-risk?	No. As discussed above, we believe standards for age appropriate content and services should be developed and online platforms should use APIs to allow on-device safety technology to direct users to the age-appropriate versions of the online platforms. This operates very well with YouTube, Google and Edge Search today. Parental controls and school safety apps can intercept requests to go to YouTube, Google/Edge Search and force a user to a maturity appropriate version (eg hiding adult content, comments or previews). Age assurance or verification is unnecessary to support this policy objective. Proposals to use age-verification gates to keep children safe make a number of unlikely or erroneous assumptions. Firstly, such a regime can only focus on a small number of online platforms. The reality is that toxicity and misbehaviour occurs vastly beyond the mainstream porn and social platforms. Secondly, teenagers will find it trivial to bypass age-verification through either VPNs or the increasing number of bio-hacks which are developing with the AI revolution. Thirdly, young children access adult content through many means other than the major porn sites. Age verification does not deal with search previews, message sharing, content shared in social & gaming platforms or inadvertent access through shared & parent devices (which will have verification tokens on them). And lastly, we believe it is ambitious to believe community support will be there for a measure which not only impacts significantly more adults than have children but will also drive concerns around privacy and tracking. The only truly reliable and effective approach to controlling a child’s online activity is by controlling the device they’re using. On-device safety technology is available today, is trustworthy and proven on 10s of millions of devices. However, this technology is being deliberately limited by

	Google, Apple and Microsoft on their own devices and compromised for 3rd party parental controls. It is not however compromised when offered to app developers (like us) to build solutions for businesses and big schools. Note, this anti-competitive and harmful behaviour has been evidenced by competition inquiries in the EU, US and Australia. When installed by enterprises, on-device safety tech can deliver all of the core needs of the UK community. Porn blocking, social media age restrictions, screentime management, visibility and alerting, are easy to use and extremely difficult to bypass. What the UK urgently needs is regulations which ensure parents have the same access to the safety technology that big enterprises enjoy. With this, there will be a fundamental upgrade of safety capability available for UK parents and schools and market forces will then ensure emerging needs are catered for. We urge OFCOM to recommend an inquiry into methods to ensure competitive and open markets for on-device technology.
Age assurance measures (Section 15)	
31. Do you agree with our proposal to recommend the use of highly effective age assurance to support Measures AA1-6? Please provide any information or evidence to support your views. a) Are there any cases in which HEAA may not be appropriate and proportionate? b) In this case, are there alternative approaches to age assurance which would be better suited? 32. Do you agree with the scope of the services captured by AA1-6? 33. Do you have any information or evidence on different ways that services could use highly effective age assurance to meet the outcome that	Absolutely no. As discussed above, we believe standards for age appropriate content and services should be developed and online platforms should use APIs to allow on-device safety technology to direct users to the age-appropriate versions of the online platforms. This operates very well with YouTube, Google and Edge Search today. Parental controls and school safety apps can intercept requests to go to YouTube, Google/Edge Search and force a user to a maturity appropriate version (eg hiding adult content, comments or previews). Age assurance or verification is unnecessary to support this policy objective. Proposals to use age-verification gates to keep children safe make a number of unlikely or erroneous assumptions.

children are prevented from encountering identified PPC, or protected from encountering identified PC under Measures AA3 and AA4, respectively? 34. Do you have any comments on our assessment of the implications of the proposed Measures AA1-6 on children, adults or services? a) Please provide any supporting information or evidence in support of your views. 35. Do you have any information or evidence on other ways that services could consider different age groups when using age assurance to protect children in age groups judged to be at risk of harm from encountering PC?	Firstly, such a regime can only focus on a small number of online platforms. The reality is that toxicity and misbehaviour occurs vastly beyond the mainstream porn and social platforms. Secondly, teenagers will find it trivial to bypass age-verification through either VPNs or the increasing number of bio-hacks which are developing with the AI revolution. Thirdly, young children access adult content through many means other than the major porn sites. Age verification does not deal with search previews, message sharing, content shared in social & gaming platforms or inadvertent access through shared & parent devices (which will have verification tokens on them). And lastly, we believe it is ambitious to believe community support will be there for a measure which not only impacts significantly more adults than have children but will also drive concerns around privacy and tracking. The only truly reliable and effective approach to controlling a child's online activity is by controlling the device they're using. On-device safety technology is available today, is trustworthy and proven on 10s of millions of devices. However, this technology is being deliberately limited by Google, Apple and Microsoft on their own devices and compromised for 3rd party parental controls. It is not however compromised when offered to app developers (like us) to build solutions for businesses and big schools. Note, this anti-competitive and harmful behaviour has been evidenced by competition inquiries in the EU, US and Australia. When installed by enterprises, on-device safety tech can deliver all of the core needs of the UK community. Porn blocking, social media age restrictions, screentime management, visibility and alerting, are easy to use and extremely difficult to bypass. What the UK urgently needs is regulations which ensure parents have the same access to the safety technology that big enterprises enjoy. With this, there will be a fundamental upgrade of safety capability available for UK parents and schools and market forces will then ensure emerging needs are catered for.

	We urge OFCOM to recommend an inquiry into methods to ensure competitive and open markets for on-device technology.
Content moderation U2U (Section 16)	
36. Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views. 37. Do you agree with the proposed addition of Measure 4G to the Illegal Content Codes? a) Please provide any arguments and supporting evidence.	No comment.
Search moderation (Section 17)	
38. Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views. 39. Are there additional steps that services take to protect children from the harms set out in the Act? a) If so, how effective are they? 40. Regarding Measure SM2, do you agree that it is proportionate to preclude users believed to be a child from turning the safe search settings off? The use of Generative AI (GenAI), see Introduction to Volume 5, to facilitate search is an emerging development, which may include where search services have integrated GenAI into their functionalities, as well as where standalone GenAI services perform search functions. There is currently limited evidence on how the use of GenAI in search services may affect the implementation of the safety measures as set out in this code. We	As discussed above, we believe standards for age appropriate content and services should be developed and online platforms should use APIs to allow on-device safety technology to direct users to the age-appropriate versions of the online platforms. This operates very well with YouTube, Google and Edge Search today. Parental controls and school safety apps can intercept requests to go to YouTube, Google/Edge Search and force a user to a maturity appropriate version (eg hiding adult content, comments or previews). Age assurance or verification is unnecessary to support this policy objective. Proposals to use age-verification gates to keep children safe make a number of unlikely or erroneous assumptions. Firstly, such a regime can only focus on a small number of online platforms. The reality is that toxicity and misbehaviour occurs vastly beyond the mainstream porn and social platforms. Secondly, teenagers will find it trivial to bypass age-verification through either VPNs or the increasing number of bio-hacks which are developing with the AI revolution. Thirdly, young children access adult content through many means other than the major porn sites. Age verification does not deal with search pre-

welcome further evidence from stakeholders on the following questions and please provider arguments and evidence to support your views: 41. Do you consider that it is technically feasible to apply the proposed code measures in respect of GenAI functionalities which are likely to perform or be integrated into search functions? 42. What additional search moderation measures might be applicable where GenAI performs or is integrated into search functions?	views, message sharing, content shared in social & gaming platforms or inadvertent access through shared & parent devices (which will have verification tokens on them). And lastly, we believe it is ambitious to believe community support will be there for a measure which not only impacts significantly more adults than have children but will also drive concerns around privacy and tracking. The only truly reliable and effective approach to controlling a child's online activity is by controlling the device they're using. On-device safety technology is available today, is trustworthy and proven on 10s of millions of devices. However, this technology is being deliberately limited by Google, Apple and Microsoft on their own devices and compromised for 3rd party parental controls. It is not however compromised when offered to app developers (like us) to build solutions for businesses and big schools. Note, this anti-competitive and harmful behaviour has been evidenced by competition inquiries in the EU, US and Australia. When installed by enterprises, on-device safety tech can deliver all of the core needs of the UK community. Porn blocking, social media age restrictions, screentime management, visibility and alerting, are easy to use and extremely difficult to bypass. What the UK urgently needs is regulations which ensure parents have the same access to the safety technology that big enterprises enjoy. With this, there will be a fundamental upgrade of safety capability available for UK parents and schools and market forces will then ensure emerging needs are catered for. We urge OFCOM to recommend an inquiry into methods to ensure competitive and open markets for on-device technology.

User reporting and complaints (Section 18)

43. Do you agree with the proposed user reporting measures to be included in the draft Children's Safety Codes? a) Please confirm which proposed measure your views relate to and explain your views and provide any arguments and supporting evidence. b) If you responded to our Illegal Harms Consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response. 44. Do you agree with our proposals to apply each of Measures UR2 (e) and UR3 (b) to all services likely to be accessed by children for all types of complaints? a) Please confirm which proposed measure your views relate to and explain your views and provide any arguments and supporting evidence. b) If you responded to our Illegal Harms Consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response. 45. Do you agree with the inclusion of the proposed changes to Measures UR2 and UR3 in the Illegal Content Codes (Measures 5B and 5C)? a) Please provide any arguments and supporting evidence.	No additional comments.

Terms of service and publicly available statements (Section 19)	
46. Do you agree with the proposed Terms of Service / Publicly Available Statements measures to be included in the Children’s Safety Codes? a) Please confirm which proposed measures your views relate to and provide any arguments and supporting evidence. b) If you responded to our illegal harms consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response. 47. Can you identify any further characteristics that may improve the clarity and accessibility of terms and statements for children? 48. Do you agree with the proposed addition of Measure 6AA to the Illegal Content Codes? a) Please provide any arguments and supporting evidence.	No additional comments.
Recommender systems (Section 20)	
49. Do you agree with the proposed recommender systems measures to be included in the Children’s Safety Codes? a) Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence. b) If you responded to our illegal harms consultation and this is relevant to your response here, please signpost to the relevant parts of your prior response.	No additional comments.

50. Are there any intervention points in the design of recommender systems that we have not considered here that could effectively prevent children from being recommended primary priority content and protect children from encountering priority and non-designated content? 51. Is there any evidence that suggests recommender systems are a risk factor associated with bullying? If so, please provide this in response to Measures RS2 and RS3 proposed in this chapter. 52. We plan to include in our RS2 and RS3, that services limit the prominence of content that we are proposing to be classified as non-designated content (NDC), namely depressive content and body image content. This is subject to our consultation on the classification of these content categories as NDC. Do you agree with this proposal? Please provide the underlying arguments and evidence of the relevance of this content to Measures RS2 and RS3. • Please provide the underlying arguments and evidence of the relevance of this content to Measures RS2 and RS3.	
User support (Section 21)	
53. Do you agree with the proposed user support measures to be included in the Children's Safety Codes? a) Please confirm which proposed measure your views relate to and provide any arguments and supporting evidence. b) If you responded to our Illegal harms consultation and this is relevant to your response here, please signpost	No additional comments.

to the relevant parts of your prior response.	
Search features, functionalities and user support (Section 22)	
54. Do you agree with our proposals? Please provide underlying arguments and evidence to support your views. 55. Do you have additional evidence relating to children's use of search services and the impact of search functionalities on children's behaviour? 56. Are there additional steps that you take to protect children from harms as set out in the Act? a) If so, how effective are they? As referenced in the Overview of Codes, Section 13 and Section 17, the use of GenAI to facilitate search is an emerging development and there is currently limited evidence on how the use of GenAI in search services may affect the implementation of the safety measures as set out in this section. We welcome further evidence from stakeholders on the following questions and please provide arguments and evidence to support your views: 57. Do you consider that it is technically feasible to apply the proposed codes measures in respect of GenAI functionalities which are likely to perform or be integrated into search functions? Please provide arguments and evidence to support your views.	Making search safe requires the search platform creating a safe version AND on-device safety technology ensuring the under-age user is directed to that service. This operates very well with YouTube, Google and Edge Search today. Parental controls and school safety apps can intercept requests to go to YouTube, Google/Edge Search and force a user to a maturity appropriate version (eg hiding adult content, comments or previews). Critical to any truly reliable and effective approach to controlling a child's online activity is by controlling the device they're using. On-device safety technology is available today, is trustworthy and proven on 10s of millions of devices. However, this technology is being deliberately limited by Google, Apple and Microsoft on their own devices and compromised for 3rd party parental controls. It is not however compromised when offered to app developers (like us) to build solutions for businesses and big schools. Note, this anti-competitive and harmful behaviour has been evidenced by competition inquiries in the EU, US and Australia. When installed by enterprises, on-device safety tech can deliver all of the core needs of the UK community. Porn blocking, social media age restrictions, screentime management, visibility and alerting, are easy to use and extremely difficult to bypass. What the UK urgently needs is regulations which ensure parents have the same access to the safety technology that big enterprises enjoy. With this, there will be a fundamental upgrade of safety capability available for UK parents and schools and market forces will then ensure emerging needs are catered for. We urge OFCOM to recommend an inquiry into methods to ensure competitive and open markets for on-device technology.

Combined Impact Assessment (Section 23)	
58. Do you agree that our package of proposed measures is proportionate, taking into account the impact on children's safety online as well as the implications on different kinds of services?	We believe they are misguided. A focus on on-device technology is absolutely fundamental to online safety. There is no practical enforcement without it.
Statutory tests (Section 24)	
59. Do you agree that our proposals, in particular our proposed recommendations for the draft Children's Safety Codes, are appropriate in the light of the matters to which we must have regard? a) If not, please explain why.	We believe they are misguided. A focus on on-device technology is absolutely fundamental to online safety. There is no practical enforcement without it.
Annexes **Impact Assessments (Annex A14)**	
60. In relation to our equality impact assessment, do you agree that some of our proposals would have a positive impact on certain groups? 61. In relation to our Welsh language assessment, do you agree that our proposals are likely to have positive, or more positive impacts on opportunities to use Welsh and treating Welsh no less favourably than English? a) If you disagree, please explain why, including how you consider these proposals could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.	No additional comments.

Please complete this form in full and return to protectingchildren@ofcom.org.uk.