

Consultation: Protecting children from harms online - Ofcom

About the Institution of Engineering and Technology (IET)

The IET is a trusted adviser of independent, impartial, evidence-based engineering and technology expertise. We are a registered charity and one of the world's leading professional societies for the engineering and technology community with over 155,000 members worldwide in 148 countries. Our strength is in working collaboratively with government, industry and academia to engineer solutions for our greatest societal challenges. We believe that professional guidance, especially in highly technological areas, is critical to good policy making.

For further details on the evidence submitted, please contact poli=cy@theiet.org.

Executive Summary

The UK's Online Safety Act (OSA) is a vital to help the UK manage technologies in a safe and regulated way, however, this is only the first step. The "duty of care" placed on tech companies, social media websites, and other businesses operating in this space aims to remove harmful or illegal content and protect children; yet there is still ambiguity from the language about the term content. As defined by the OSA, content should include immersive reality platforms.

We have consistently campaigned to raise awareness of the huge potential, yet also the significant harms that can occur in virtual reality (VR) through our briefings to Lords during the Online Safety Bill's progress through parliament and once the bill had gained royal assent. Despite assurances that the OSA regulates to cover the metaverse, persistently, language around online safety is still too focussed on 2D interaction and not immersive behaviour. It is also pivotal that further research is undertaken into the distinctions between 2D and immersive environments and the impact that this has for regulation.

Recommendations:

- **Immersive technologies** should be given specific consideration in regulation so that there is no ambiguity for users and businesses about the legality of actions that take place in virtual reality. Although they differ to the ‘traditional’ forms of social media, they can be just as harmful to their users.
- **Future refinement and further clarification are needed.** There is scope for further refinement and clarification of the proposals. For example, defining more specifically a “significant number of children”.
- **Continuous review and improvement:** The best way to tackle online harms to children and ensure the proposals maintain up to date and effective will be to continually review, scrutinise and improve them accordingly. A review should be undertaken into the impact of the OSA on regulating immersive reality.
- **Choice and support.** Clear and accessible information, with an easy-to-use reporting and complaints processes, is essential to the success of protecting children from online harms.

Age assurance, child user condition, and interpretation of “significant number of users who are children”

The IET agrees with the 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. This proposal ensures that a child’s access is restricted effectively and that services are taking appropriate measures to protect children from accessing unsuitable content.

Future measures should consider the potential impacts on service providers, especially SME’s. While most services will likely conclude that they are accessible by children, this could result in cost implications for small, low-risk services due to conducting a children’s risk assessment and taking appropriate steps to comply with the children’s safety duties.

Almost two thirds (62%) of parents of children aged 5-10 don’t currently understand the metaverse, highlighting the need to safeguard this new space. However, despite the lack of understanding, more than a fifth of 5 – 10-year-olds already have a VR headset of their own or have asked for a similar tech present for their birthday or Christmas. 15% of them have already tried VR, and 6% use it on a regular basis.

But there is apprehension from parents as well as a lack of knowledge. Only 10% of parents feel comfortable letting their child explore the metaverse through VR without supervision. Of those parents whose children already interact with VR, over a quarter admitted they did not know what their child was accessing in this new virtual world, underlining the need for robust safeguarding to be introduced¹.

Future measures could further clarify the interpretation of "significant number of users who are children" and the factors considered when assessing whether the child user condition is met.

Children's access assessments

Further refinement of the process for children's access assessments should be considered. This involves determining whether a service or a part of the service is likely to be accessed by children. Services likely to be accessed by children must comply with the children's risk assessment duties and the safety duties protecting children.

Causes and impacts of online harms

Although the OSA helps the UK reap the benefits of new technologies in a safer, more regulated way, the lack of inclusion of immersive technology proves that it doesn't go far enough. While some safety measures for immersive environments may overlap with those for apps and websites, others necessitate distinct approaches.

Most internet usage still involves users gazing at and engaging with a luminous rectangular display. Immersive technologies inherently differ from traditional social media platforms and the World Wide Web. Immersive environments aren't platforms for content consumption; they serve as arenas for real-time activities, augmented reality (AR) and VR allow users to step inside it, actively participating instead of merely observing, listening, or inputting information. Users immerse themselves

¹ The IET (2022), Generation VR. <https://www.theiet.org/media/press-releases/press-releases-2022/press-releases-2022-april-june/19-april-2022-generation-vr>

physically, via haptic suits, thereby transcending the limitations traditional online engagement.

There are serious crimes being committed in the metaverse, through use of haptic suits, for example: one of the most popular VR pornography experiences available is *After School Girlfriend*. It is built for the Meta Quest and is available through 'sideloading' (an unofficial source). Users can simulate sex with a schoolgirl in a range of environments, users can also use this experience to replicate harassment and abuse including sexual abuse, grooming and exploitation of children. Coupled with this, there is ambiguity surrounding criminal accountability for individuals and publishers/platforms, therefore, making it difficult to prosecute those accountable.

Similar to the real world, events unfold directly within VR – users immerse themselves into them. Harms in these digital forums are human-to-human, interpersonal behaviours. Activity here is 'conduct' as 'content', and when negative experiences occur, it is similar to the experience of something happening in the real world. Therefore, regulations and legislation must acknowledge and account for this pivotal distinction – and that laws work to prevent serious harms that are already too prevalent in the metaverse.

As well as this, we have concerns around voice/translation services. Voice and translation services, and the possible manipulation of these services, need to be addressed in the OSA. There are obvious keywords that would qualify as 'age inappropriate' words, but we are unsure if there is anything in the OSA that can protect users from online translation of voice, a topic which has potential to be mainstream within the next 24 months. We think there is scope for this to be analysed and for it to be covered in the OSA, in order to protect various VR and online users.

For further information, please see, [Safeguarding the Metaverse](#)² report in 2022 highlighting the potential issues that need addressing in immersive reality. This report was authored by immersive tech experts Catherine Allen and Verity McIntosh.

Age groups for assessing risk by age

The service providers should use highly effective age assurance techniques to ensure that children are not able to access the services. This can prevent children from accessing the entire service to fulfil children's safety duties.

Risks to children from GenAI content or applications on U2U or Search services

Generative AI (GenAI) content poses similar threats to that of VR and 3D content. It can be very harmful and very hard for parents to supervise. Ofcom has a critical role in regulating this space to prevent serious harms that are already prevalent in the metaverse³

Large vertical search services are unlikely to have content that is rapidly changing as User-to-User (U2U) and search results are more under a service's control for U2U content. The consultation document also mentions that there is no known evidence of such services showing content harmful to children, which lowers the potential for unidentified risks.

Given the importance of tracking new and increasing risks to children, measures are being identified for inclusion in the Children's Safety Codes. It implies an ongoing effort to identify and manage risks to children, but it does not specifically mention GenAI content or applications.

For the aforementioned reasoning, any GenAI content, either text or specifically generated imagery, should include watermarks or another simple method of identification for children/users so they can know that the content is artificially

² The IET (2022), Safeguarding the metaverse <https://www.theiet.org/impact-society/factfiles/information-technology-factfiles/safeguarding-the-metaverse>

³ The IET (2023). IET comments on the Online Safety Bill [https://www.theiet.org/media/press-releases/press-releases-2023-july-september/20-september-2023-iet-comments-on-online-safety-bill](https://www.theiet.org/media/press-releases/press-releases-2023/press-releases-2023-july-september/20-september-2023-iet-comments-on-online-safety-bill)

generated and not real. This would be beneficial in numerous ways, not least the debunking of fake news/imagery that may be used to indoctrinate children. There is some false posts on various social media platforms that may evade the 'graphic' title, but may still influence its viewers.

To summarise, based on the provided sources, there is no specific mention of risks to children from GenAI content or applications on U2U or search services. However, there are measures being put in place to track and manage new and increasing risks to children.

Four-step risk assessment and the Children's Risk Profiles

There are several key points highlighted in the 'Vol 4 – Assessing the risks of harms to children online' document including emphasis on the need for services to establish a baseline understanding of the frequency of particular kinds of content appearing on their service. The document also refers to proportionality. This provides flexibility for services to conduct risk assessments in a cost-effective and manageable way. This benefits particularly SME's that have few or no relevant risk factors. However, larger services or services with many risk factors are expected to incur more substantial costs, which is considered necessary by the Act for such risk assessments to demonstrate that they are suitable and sufficient.

Future measures for the Children's Safety Codes

Services need to keep their children's access assessments, risk assessments, and safety measures up to date. The document also suggests that service providers monitor the effectiveness of the safety measures they implement and continually improve them over time, which is welcome.

The Act requires that proposals are proportionate. While a higher level of protection is needed for children than for adults, it's also important to ensure that children retain the benefits of being online. In assessing the proportionality of Codes measures, the primary consideration is the extent to which they can reduce risks of harm to children, taking into account both the scale and severity of harm. Cost is not a sufficient reason for providers not to take measures.

There should be more choice and support for children, for example, ensuring clear and accessible information for children and caregivers, with easy-to-use reporting and complaints processes, and giving children tools and support to help them stay safe. For instance, children will not normally be able to access inappropriate content, they will be protected from seeing, and being recommended, potentially harmful content, they will not be added to group chats without their consent, and it will be easier for them to complain when they see harmful content.

Conclusion

Although the UK Online Safety Act is a vital piece of regulation to help the UK benefit from new technology in a safe and regulated way, current measures do not go far enough to mitigate harm both now and in the future, as technology progresses. The language around online safety is still too focussed on 2D interaction and not immersive behaviour, causing ambiguity.

It is pivotal that immersive technologies are specifically outlined in the proposals set out in this consultation, as they can be just as harmful to their users as 'traditional' forms of social media can be.

Despite the proposals being a step in the right direction in protecting children from online harms, further refinement and clarification are needed if it is to take full effect. This will come from continually reviewing and improving the various assessments, proposals and the impact that they are having. This will ensure the proposals maintain up to date and effective.

Finally, for these proposals to also succeed, collaboration with parents/caregivers is vital. Therefore, providing a choice and support for children, accompanied by clear and accessible information, with an easy-to-use reporting and complaints processes, will make tech companies and various digital platforms accountable for harmful content on their servers.