Statutory report on content harmful to children call for evidence

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 158,000 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.

Executive Summary

The Institution of Engineering and Technology (IET) welcomes the opportunity to respond to this call for evidence to support the first statutory report on content harmful to children. The IET commends the progress made already by Ofcom whilst implementing the OSA.

Technology moves at a fast pace, and therefore managing the subsequent harms to children and other vulnerable people requires agility and constant review. The IET advises that instead of responding on a case-by-case basis to new technologies, regulation should take a technology forward approach in addition to existing measures. Technology will advance quickly, affecting every aspect of life, largely for the better, and so to manage inevitable misuse of technology, we should look at safety through the lens of the technology itself instead of seeking to overly limit or restrict it. The IET recommends several ways to do this, for example, enhancing digital skills in children, supporting parents to understand the ways they can use parental controls and by increasing the ability to expunge data from the internet. Measures such as restricting the use of VPNs come with a negative knock-on effect for cyber security in businesses, an area the UK is currently trying to increase its resilience on.

The IET also reiterates the urgent need for immersive technologies to be treated as a distinct area of regulatory focus due to the unique risks they pose to children and vulnerable users. Drawing on the expertise of our members, we outline the challenges of age verification, the prevalence of unsupervised minors in virtual reality (VR) spaces, and the embodied nature of harm in these environments. We call for targeted action to ensure that immersive platforms are safe, transparent, and accountable, and that regulation continues to evolve in step with technological advancement and virtual reality. Despite its prevalence, virtual reality remains a grey area, even though it was defined clearly as content in the OSA. This is likely to further escalate with the development of wearable technology that links to social media and immersive platforms.

There should be a greater focus on preventing harms to children and vulnerable people using technology itself, the IET recommends:

- **Wide-reaching definitions for technology:** There needs to be an inclusion of a wide-reaching definition of "user", "content" and "agency" when talking about technology.
- **VPNs**: There should be caution over general bans on VPNs when putting into effect the age limitation legislation. VPNs are an important tool for businesses to ensure

cybersecurity safety; a general ban has the potential to have a knock-on effect of cyber resilience in the economy.

- **Digital Skills:** Children must be protected but still develop digital skills. Policies in this area should be forward thinking, not responsive to incidents on a case-by-case basis.

- **Legislation:** The UK's OSA was a vital first step to help the UK manage technologies in a safe and regulated way. However, 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 pivotal that further research is undertaken into immersive environments and the impact that this has for regulation. A review should be undertaken into the impact of the OSA on regulating immersive reality. (IET, 2024, Protecting children from harms online).

- **Institutions:** Professional bodies should support Ofcom in ensuring compliance of metaverse providers. Providing a safe process for whistle blowers and responding meaningfully to user complaints (IET, 2022, Safeguarding the metaverse).

- **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 (IET, 2024, Protecting children from harms online, 2024).

- **Parental controls:** There should be greater support to parents to understand how to limit and control access to certain content on their devices within the home and school environment.

- **Data:** There should be the ability to expunge your data from social media, for example on behalf of a child, or once the child reaches 18.

Future Proofing

There are already gaps within legislation, for example, chatbots, which the government is urgently trying to address. There needs to be a wide-reaching definition of 'user', 'content' and 'agency' when considering online safety, especially with the rise of AI and deepfakes. Going beyond traditional definitions and interpretations of who is considered a user is important to understand the harms caused by misuse and manipulation of AI.

There needs to be greater focus on improving safety through technology itself, such as support for greater parental controls to manage access to content and, for example the right to expunge data records on behalf of a child. Measures to improve safety through technology should be done by regulators and government working in close partnership with developers to understand the emerging technologies and build in safeguards at an early stage.

The IET recommends caution over general bans on VPNs, when putting into effect the age limitation legislation. VPNs are an important tool for businesses to ensure cybersecurity safety; a general ban has the potential to have a knock-on effect of cyber resilience in the economy.

Children must be protected but still develop digital skills. Policies in this area should be forward thinking, not responsive to incidents on a case-by-case basis. For example, regulators should look to future technology trends, such as wearables, and the impact they might have on privacy, social media in VR, deepfakes, AI content generation and personal data.

Regulation in the Metaverse

It is important to highlight the growing challenges of regulating behaviour within virtual reality environments. While the OSA marked a substantial step forward in addressing digital harms, and despite ongoing efforts to address these challenges, significant gaps remain in its ability to protect users from exploitation and abuse. As immersive technologies become more common, the complexity of monitoring and enforcing standards in these spaces presents significant hurdles, especially when it comes to safeguarding children and vulnerable individuals online. The immersive environment offers a wide range of opportunities for users to benefit from the experience such as simulating training in high-risk scenarios such as nuclear power plants. When a user participates in virtual reality, the experience is one not just of viewing, but of immersive interaction. As a result, the boundary between virtual and real-world interaction becomes blurred. The vast opportunity that virtual reality and the metaverse presents can only be captured if the safety, dignity and rights of end-users are protected.

While virtual reality is often perceived as a family entertainment device, most consumer headsets have a lower age limit of either 12 or 13. This is written into the manufacturer's terms and conditions, with the main route to enforcement being through the linking of the headset to an online account elsewhere in which the user's date of birth has already been required. There is consensus among industry experts and researchers that the lower age limit is not widely adhered to. IET research showed that 25% of children aged 5-13 are using virtual reality on a weekly basis, and that young peoples' engagement with VR had grown by 320% in 2022 (E&T Magazine, 2023, Children spend more time online than in the real world).

The evidence gathered for the "Safeguarding the metaverse" report in 2022, highlighted that in multi user virtual reality spaces that unsupervised children participated in openly accessed virtual reality spaces. This included under 13-year-olds and over 13-year-olds (the mandatory lower age limit for virtual users). In these spaces the authors met children that were as young as six, meaning that children are interacting with adult strangers. What makes this situation different to non-immersive media, such as chatrooms, is that virtual reality is embodied. Users can not only interact verbally, but also physically, which are represented by avatars. On VRChat, one of the most popular metaverse apps on the Meta Quest, avatar nudity was observed.

Research from the Centre for Countering Digital Hate (CCDH) shows that VRChat is "rife with abuse, harassment, racism and pornographic content". CCDH researchers found that users, including children, are on average exposed to abusive behaviour every seven minutes. Abusive behaviour recorded and reported by CCDH researchers included:

1. Exposure to graphic sexual content.
2. Bullying, sexual harassment and abuse of other users, including children.
3. Minors being told to repeat racist slurs and extremist talking points. (IET, 2022, Safeguarding the metaverse).

Conclusion

To future proof and keep pace with technology, we must broaden the definitions we have traditionally used and seek to manage technology more through the use of technology. Technologies are on the horizon that pose new risks to the safety of vulnerable people and it's important to consider the impact that they might have before they become common use, everyday items. Immersive technologies are reshaping digital interaction, but without robust safeguards, they risk becoming environments that allow abuse and exploitation. The IET urges Ofcom to address virtual reality, AI and deepfakes, and immersive wearables for regulatory focus, particularly in regard to the safety of children and vulnerable people.

The IET would welcome the opportunity to provide further advice or expertise on this subject, if this would be useful, please contact policy@theiet.org to arrange a meeting and discuss further.