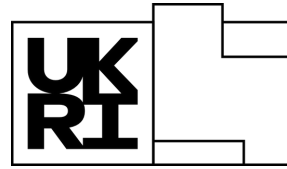




**Innovate  
UK**



**Innovate UK**  
IMMERSIVE TECH  
NETWORK



# **Innovate UK Creative Catalyst**

**Tackling Immersive Technology Harms:  
What You Need to Know, Now**





## Introduction

In collaboration with the Innovate UK Immersive Tech Network, the Innovate UK Creative Catalyst Peer Network hosted the Tackling Immersive Harms summit, to explore the harms end users may face when using immersive technologies, and how these might be tackled by the sector. This event was inspired by the scoping work undertaken between 2023-2024 by the Innovate UK Immersive Tech Network to develop and set up the Ethics Working Group.

As immersive technology enters the mainstream, users and the wider public are becoming increasingly aware of the potential harms that Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR) might facilitate. Many people are understandably anxious about these technologies, having witnessed the various negative impacts of earlier technologies like social media. Issues like grooming and harassment in virtual spaces have entered the forefront of public consciousness.

Change is on the horizon, though. Legal requirements to address illegal online harms in the UK came into force in March 2025, under the Online Safety Act, which includes immersive technologies. Ofcom, as the communications regulator, has been tasked by Parliament with enforcing the Act and now requires organisations covered by the Act to comply with illegal content safety duties.

## INDUSTRY INSIGHTS AND REFLECTIONS

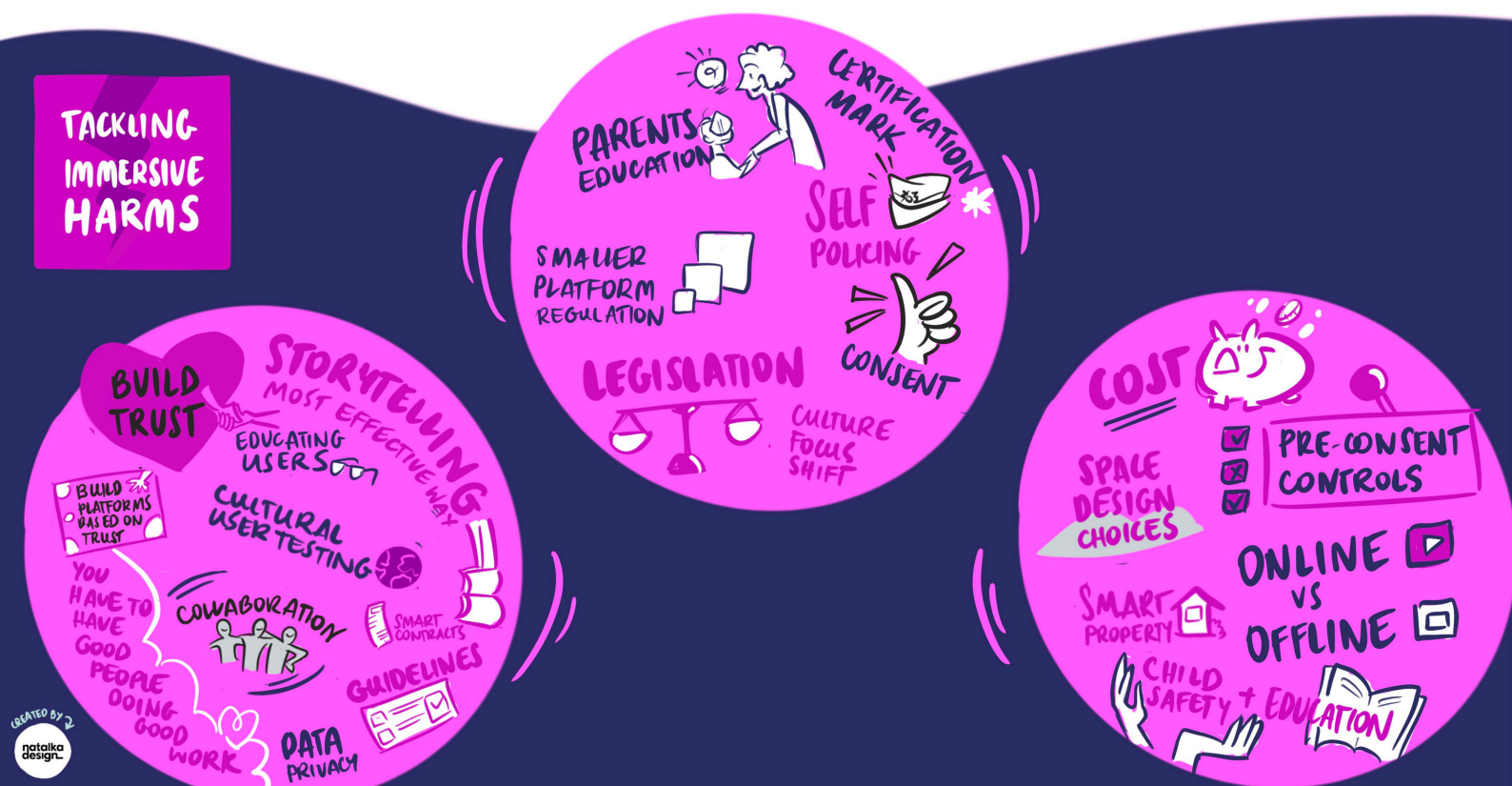


Figure 1. Tackling Immersive Harms event – A visual doodle by Nataalka Design capturing key industry insights and reflections shared during the session.

Many immersive sector companies will fall under the remit of the act and will need to comply. However, regardless of being in scope of this law, many immersive sector organisations are seeking to address these issues independently as they understand the importance of tackling problems early on in the medium's development.

The summit explored what immersive businesses need to know now about the harms and regulatory changes, as well as investigating possible industry-led solutions to the challenges presented. The event brought together world leading experts in this field, with representation from Interpol, The Information Commissioner's Office, leading academics specialising in the field and key industry voices.





The event brought together world-leading experts in this field, with representation from:

- Catherine Allen, CEO and Lead Consultant, Limina
- Emma Barrett OBE, Professor of Psychology, Security and Trust, The University of Manchester
- Stephanie Baxter, Head of Policy, Institution of Engineering and Technology, IET
- Christopher Church, Senior Forensics Specialist at INTERPOL
- Professor Julia Davidson OBE, PhD, Director Institute for Connected Communities and Executive Director of Research, University of East London
- Verity McIntosh, Associate Professor of Virtual and Extended Realities, University of West of England
- Dr Lynsay Shepherd, Reader in Cybersecurity and Human-Computer Interaction, Abertay University
- Alice Trotter, Associate, Kingsley Napley LLP

This paper, written by leading immersive industry specialist, Catherine Allen, CEO and Lead Consultant at Limina Immersive, draws from the event's findings summarising what you need to know now about existing and future harms and how, as a sector, we can begin to tackle them. The findings from this event will feed into the ongoing work being done by the Innovate UK Immersive Tech Network Ethics Working Group, which officially launched in March 2025.





## Existing and potential harms facilitated by immersive technologies

Like with any new innovation, immersive technologies offer both opportunity and threat. It is often not until major safety problems have been solved that innovations can truly ‘take off’ and reach the mainstream.

Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR) can offer groundbreaking ways to interact, communicate, and create, however they also bring significant risks that those from industry attending the summit agreed must be addressed, from both an industry growth and end-user safety perspective.

The current landscape of harms explored at the summit included:

# Existing and potential harms



## Privacy and security risks:

- Concerns around data collection, including biometric data and physical activity
- Lack of transparency and user control over how this data is collected, used, and shared
- Challenges around meaningful user consent for data usage
- Potential for highly effective targeted marketing and profiling based on this granular behavioural data
- Questions around user's "cognitive liberty" and right to mental privacy in these environments.

---

## Fraud and financial crimes:



- Identity theft and impersonation fraud
- Account takeover attacks
- Frauds, including potential for money laundering - exacerbated due to unclear jurisdictions
- Highly effective romance scam.

---

## Physical and psychological harms:



- Sexual abuse including VR 'deep fakes' and underage access to VR pornography
- Physical safety risks like eye strain, nausea, and crashing into walls and furniture
- Potential for haptic technology to be used to cause physical assault
- Risk of deliberately inducing trauma, false memories, and psychological distress.



# Existing and potential harms



## Harms to children and vulnerable users:

- Sexual grooming, exploitation, and abuse, including of children
  - Exposure to inappropriate or harmful content
  - Isolation, addiction, and other wellbeing impacts
- 



## Governance and accountability:

- Ambiguity around who is responsible for enforcing safety and moderating content in immersive spaces
  - Challenges of applying existing laws and regulations to virtual environments that may exist outside traditional jurisdictions.
- 



## Other societal harms:

- Intense spread of misinformation and disinformation
- Potential for use by extremist or terrorist groups, for instance to train and recruit
- Issues around discrimination and bias in AI-powered experiences Environmental impacts from the energy usage of these technologies.




Of all the issues discussed, one that appeared most immediately prevalent was harassment within multi-user virtual environments. Unlike social media, where abuse often takes place via text or image-based exchanges, harassment in immersive spaces is experienced in real-time, much like in real life. Julia Davidson, Professor of Criminal Justice and Cybercrime and Executive Director of Research at University of East London, shared findings of her research showing children reporting incidents of racial abuse, sexual harassment, and unwanted contact – experiences that can feel just as real and traumatising as physical-world situations. The anonymity provided by avatars and the nascent state of platform moderation tools exacerbate these issues, making it difficult for victims to seek recourse.

Another critical area of concern discussed involves privacy and data security. Immersive environments collect more granular behavioural data than most other technologies. They can track eye movement, physical gestures and voice characteristics, often without the user's explicit awareness. This level of data collection opens up new risks for misuse.

The exploitation of behavioural biases through "dark patterns" – design elements that nudge users towards specific actions – was noted as a particular concern, as was the potential for immersive technologies to encourage unhealthy behaviours by keeping users engaged for extended periods.





The potential rise of hyper-personalised scams was another significant point of discussion. In immersive environments, the depth of personal and behavioural data available means that scams can be tailored to exploit individual behaviours and interactions, making them harder to detect and more effective.


Several speakers at the summit highlighted evidence of virtual reality being exploited for sexual abuse, particularly targeting women and children. The NSPCC commissioned reports co-authored by Catherine Allen and Verity McIntosh that were discussed identified specific harms such as sexual grooming, harassment, and underage access to VR pornography. Professor Emma Barrett noted the potential for the immersive and embodied nature of VR to enable new forms of sexual exploitation and abuse that can have severe psychological impacts on the victim. Professor Julia Davidson's study with young people revealed they had already encountered cases of sexual harassment in the metaverse. Lawyer Alice Trotter provided a disturbing example of a minor being virtually "attacked" in a VR game, suffering trauma akin to physical sexual assault.

As well as these topics, the industry roundtable sessions explored the potential environmental impact of immersive technologies, including the increased demand for internet infrastructure, energy consumption, and the materials needed to produce headsets and other hardware.

Participants emphasised the importance of considering these environmental factors to ensure that the development of immersive technologies does not come at an unsustainable cost to the real-world environment, especially when immersive experiences are combined with AI.

Finally, there is the potential harm of misinformation in immersive environments spreading unchecked. As the psychological boundaries between reality and virtuality blur, misinformation can have a heightened impact – potentially making it easier for users to accept false narratives.

There has been research demonstrating the capacity for VR to both illicit false memories as well as being extreme persuasive – with the potential to change the real-life behaviour of end users\*.





## How these harms can be tackled

Immersive technologies are powerful and can be used for incredibly positive results, but they can also be misused, leading to a cascade of negative effects on individuals and society. Addressing these ethical challenges early is vital in ensuring that society gets the best out of immersive tech's capabilities.

## Challenges in traditional forms of law enforcement

A significant obstacle in addressing these harms in immersive environments is the difficulty in applying traditional law enforcement techniques. There are many reasons for these difficulties, from lack of knowledge and confidence in police forces to anonymity making perpetrators very hard to identify.

---

\*The persuasive power of virtual reality: effects of simulated human distress on attitudes towards fire safety  
Designing for Persuasion through Embodied Experiences in Virtual Reality  
Increasing saving behaviour through age-processed renderings of the future self





Christopher Church from Interpol also explained how the borderless, decentralised nature of virtual worlds can create jurisdictional issues, as crimes can involve perpetrators, victims and platforms across different countries.

On top of this, the lack of physical evidence makes it hard to build robust legal cases; lawyer Alice Trotter noted that existing laws were simply not written with virtual crimes in mind.

This creates an ambiguity around how laws apply. For instance, concepts like "physical touching" in sexual assault laws do not easily translate. These issues that law enforcement teams face make it hard for immediate solutions to come from these more traditional avenues.

This places even more of an onus on the immersive sector; industry-led solutions have the potential for rapid change that comes from a position of really understanding the technology and its capabilities.

## Industry-led solutions

The event's round table sessions highlighted a clear appetite for taking a proactive, collaborative approach to addressing the ethical and safety challenges of these emerging platforms.

One key proposal was the development of voluntary industry standards and certification schemes. Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR) apps, for instance could have a quality mark, akin to the CE and UKCA marks on consumer products to ensure safety. By coming together to establish baseline safety practices, platforms and applications could give users greater confidence in the security and safety of different virtual apps and environments.

A code of conduct for companies was also discussed, with the underpinnings of this code being a concerted effort to build trust with users through transparent data practices, clear quality testing and, when the experience is multi-user, robust moderation.

Roundtable participants also shared how they felt it was equally important to start from the adaptation of real-world behavioural principles – after all, the medium that immersive media is most like is the real world. Inspiration ranging from proxemics to theatre practices could guide the design of immersive environments.

Another solution discussed was along the theme of data sovereignty: the implementation of consent controls and identity verification frameworks that could be applied across multiple immersive platforms. This could involve the sector developing interoperable systems that allow people to manage their personal information and privacy preferences in one place as they use different XR apps and environments. Rather than being beholden to the data policies of a single dominant platform, users would own their own data and have the ability to pre-set consent parameters and identity verification methods that travel with them.

This portability of user controls would create a baseline of trust around data gathering that would give users an underlying sense of security when they put on a VR headset or AR glasses.





Finally, industry-wide educational initiatives were identified as both a strong and feasible step forward. These initiatives could include awareness campaigns to inform users about how to stay safe in immersive environments, as well as training programs for developers on ethical design practices.

## The requirements of the Online Safety Act (OSA)

The Online Safety Act (OSA) is something immersive companies need to pay close attention to, especially as it applies directly to the services many offer. With the OSA now in force since March 2025, Ofcom is taking a phased approach, with the first new duties expected shortly. Now is the time for immersive sector companies to get prepared.

## Key duty: risk assessment

The OSA applies to various categories, including user-to-user services, search services, and adult content. For most immersive companies, user-to-user services will be the most relevant category. If you are creating VR with a social component, this new law applies to you, and you fall under the user-to-user services category. The rules apply to organisations of all sizes, from large, well-resourced companies to very small "micro-businesses." Even individuals running an online service are included in the scope of the OSA. However, the actions you will need to take to comply with the OSA will vary in magnitude depending on the size of your user base, the risks involved, and the scale of the service you provide.

## Scope of the Online Safety Act

Central to the Online Safety Act is the duty of risk assessments. This means that businesses are now expected to:

- 1. Assess the risk of harm:** Understand the risks of illegal content on your platform and evaluate any risks that may be posed to children if your service is likely to be used by them
- 2. Manage and mitigate risks:** Take effective steps to manage the risks identified in these assessments. Ofcom have published codes of practice that companies can use as a guideline to implement safety measures.
- 3. Transparency for users:** Clearly communicate in your terms of service how you intend to protect users
- 4. Reporting and complaints:** Ensure users have a way to report illegal or harmful content, and provide a transparent complaints process for instances where posts have been unfairly removed or accounts have been blocked
- 5. Freedom of expression and privacy:** When implementing safety measures, you must consider how to protect freedom of expression and users' right to privacy.





Figure 2. Tackling Immersive Harms event – A visual doodle by Nataalka Design capturing the key topics discussed during the session, including industry reflections on safety, ethics, regulation, user wellbeing and the future of immersive technologies. The illustration highlights insights from a range of sector voices and collaborative approaches to addressing immersive harms.

## Preparing for compliance

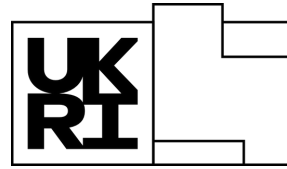
It's important for companies to start assessing the risks their platforms might present and decide on appropriate safety measures now. Ofcom will publish a range of resources, including guidance and codes of practice, to help companies understand risks and ensure compliance. The first code will be enforced from March 2025.

Overall, the tackling Immersive Harms Summit had a strong sense of proactive, fresh energy across the industry participants present – a real desire to understand the landscape of these challenges and to tackle issues head on. However, this is just the start. More vital conversations need to be had. The next step is to embed ethical practice deeply into the culture of the entire immersive technology sector. With changes in the law and public sentiment, now is great time for the growing immersive sector to keep the conversation going and implement innovative solutions to these challenges.

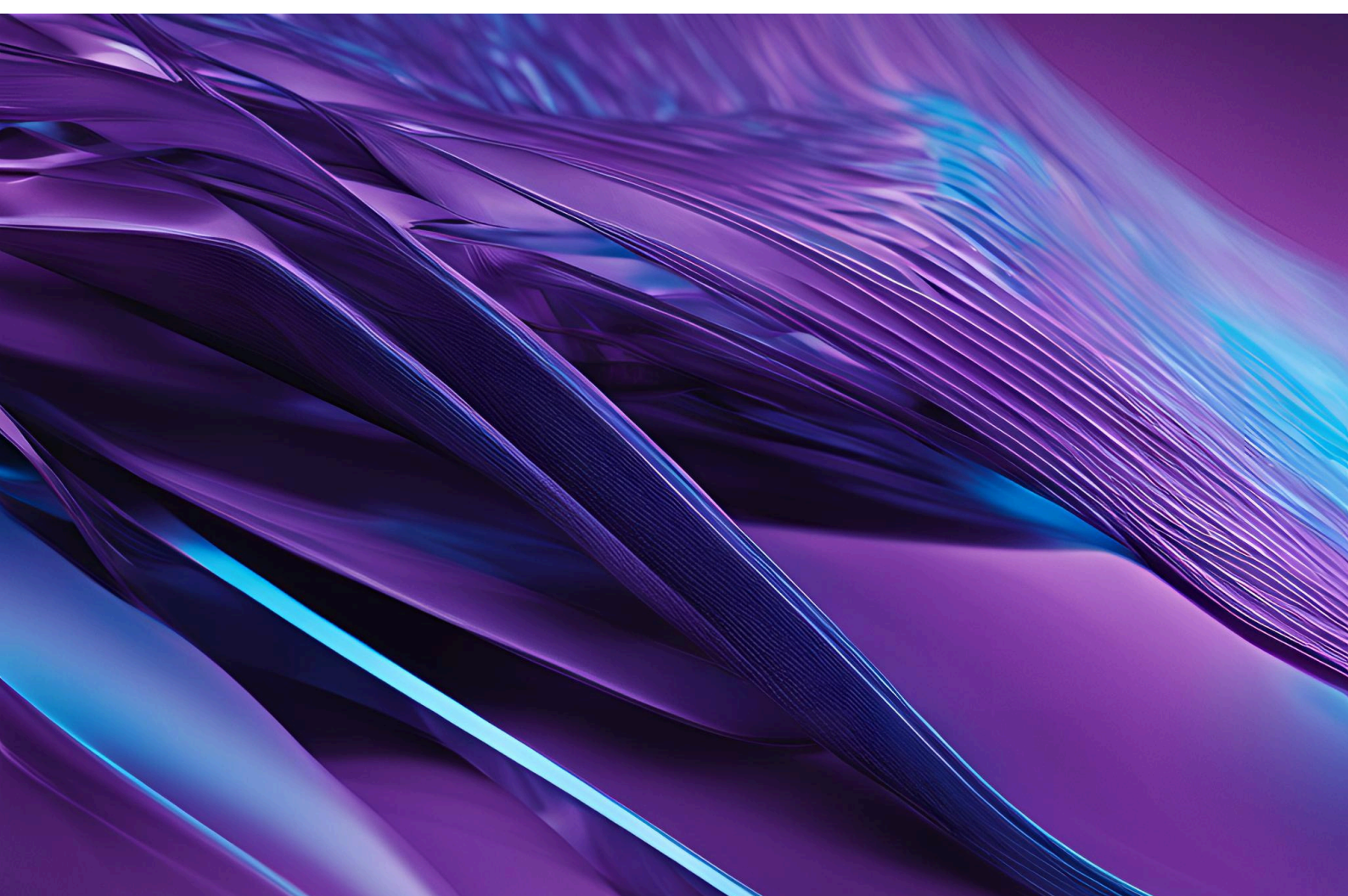




**Innovate  
UK**



**Innovate UK**  
IMMERSIVE TECH  
NETWORK



**Join our thriving  
community of business  
innovation.**

For more information about how Innovate UK can support you or  
your business, visit our website or contact us on:

**0333 340 3250    [iuk-business-connect.org.uk](https://iuk-business-connect.org.uk)**