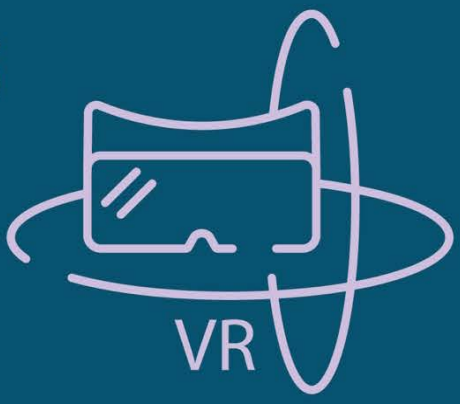
NSPCC

Child Safeguarding and Immersive Technologies

An outline of the risks



Outlining and tackling CSA and CSE harms to children in VR and the metaverse

By Catherine Allen, Limina Immersive
Commissioned by NSPCC

LIMINA IMMERSIVE

Child Safeguarding and Immersive Technologies

An Outline of the Risks

Outlining and tackling CSA and CSE harms to children in VR and the metaverse

By Catherine Allen, Limina Immersive
Commissioned by the NSPCC

Advisor and contributing author: Verity McIntosh
Editor: Sian Norris
Research: Verity McIntosh, Catherine Allen, Joanna Henderson and Emma Hughes

Contents

Content advisory

This paper includes content that tackles the issue of child sexual abuse (CSA) in Virtual Reality and immersive environments.

Some of these harms may be new information for the reader. They may be challenging to learn about and take time to process. There are parts of this paper that readers might find upsetting.

Please be aware of this content advisory warning before taking the decision to read on. We also ask you are mindful of this context if you choose to share this document with colleagues.

We also recommend that you consider your own context in which you read this paper, including time and place. If you are concerned about the wellbeing of a child, you can contact the NSPCC's Helpline to speak with a dedicated child protection specialist who will be able to provide you with free advice, support, and take action. If your child needs more support, the NSPCC's Childline service provides a safe, confidential place for children to speak with trained counsellors at any time.

About the paper

The NSPCC's 2021–2031 organisational strategy has three impact goals we want to achieve by 2031:[1]

1. Everyone plays their part to prevent child abuse

2. Every child is safe online

3. Children feel safe, listened to and supported.

Given the rapid growth of new technologies, including immersive environments, the current generation of extended reality products – Virtual Reality (VR) and Augmented Reality (AR) – and the clear shift towards the development of the metaverse, research is necessary to ensure that the safeguarding community has a clear understanding of the emerging potential impacts of such products.

The NSPCC commissioned Limina Immersive to research the CSA risks in emerging technologies, which would help us identify how these risks might effectively be mitigated.

This paper aims to inform readers on the harms to children identified in the metaverse, and support dialogue around the necessary interventions needed to mitigate risks to children in immersive environments. To build a better understanding of the key concepts in the immersive technologies, please see our supplementary paper *Child Safeguarding & Immersive Technologies: Key Concepts*. **These papers are contextual pieces prepared to provide thought leadership, in this rapidly growing sector, by reflecting the available evidence and experience of the researchers.**

Note on reading from the NSPCC

The paper explores sensitive issues and has been carefully composed to minimise, as far as is possible, graphic or triggering content for the reader, while not compromising on revealing the harms to children posed by immersive technology.

In order to protect the identity of victims, and to avoid triggering or unnecessarily upsetting readers, the NSPCC has taken the decision to paraphrase some quotes from individual users, unless those quotes already exist in the public sphere – such as having appeared on BBC News or a widely watched YouTube documentary. Where this paraphrasing happens, it is clearly labelled.

The evidence collected in the writing of this paper was unprecedented and posed safeguarding risks to the project team. There were also the risks considered in potentially signposting would-be offenders to platforms they may then go on to offend in. Due to these risks, the NSPCC has taken the decision in some places not to include the names of specific platforms or products. Further, we recognise that while some users of immersive technology platforms are engaging in harmful and exploitative behaviour, most are not and simply enjoy using VR and AR for a range of experiences. We do not wish to place any stigma on the latter groups of users.

Some sources have been kept confidential for security reasons.

While the majority of references to external research and articles are included in this paper, there are occasions where references have been removed, as they point to harmful content, or content that could reveal the identity of victims. References to these materials can be made available on request, subject to review. For access to references please contact emergingtech@nspcc.org.uk with the subject "Child Safeguarding & Immersive Technologies: An Outline of the Risks – reference request." Please include your name, organisation details, and an outline of the purpose of your request.

About the paper authors

Catherine Allen
Limina Immersive

Catherine Allen is the Founder, CEO, and lead consultant at Limina Immersive. Catherine is most well known as a UK leading expert in immersive technology and its relationship with the public. Catherine co-authored the Institution of Engineering and Technology report, *Safeguarding the Metaverse* (2022).[2] Catherine has also authored several seminal public reports that have influenced policy, for instance the *Immersive Content Formats for Future Audiences* (2018)[3] report, for Innovate UK and Digital Catapult. Catherine's insights having been featured in The Sunday Times, BBC News, Radio 4's Today Programme, Wired Magazine, British Vogue and Bloomberg. Catherine is also one of Creative England's officially recommended consultants.

Before founding Limina Immersive, Catherine led the creation of two of the BBC's first virtual reality experiences in 2015–2016 and worked on the BAFTA-winning children's app, Disney Animated.

Verity McIntosh
University of the West of England

Verity McIntosh is Associate Professor of virtual and extended realities at the University of the West of England. Verity co-authored the Institution of Engineering and Technology report, *Safeguarding the Metaverse* (2022). She is currently working with UK government and the Council of Europe to develop governance frameworks that support positive human experiences in the 'metaverse'. Verity is a member of the Digital Cultures Research Centre. Her research focuses on the ethics of presence, access and inclusion in immersive experiences, multi-person virtual experiences, and the simulation of unsafe spaces in VR. Verity has written and spoken about immersive tech and the 'metaverse' around the world, including BBC World Service, ITV News and The Sunday Times

Acknowledgements

The NSPCC is an independent charity funded overwhelmingly by voluntary donations. The NSPCC is very grateful for the generous support from the Oak Foundation who made this research possible.

With special thanks to all those who have contributed to our study, including:

- UK National Policing Online CSAE Covert Intelligence team
- Government Communications Headquarters (GCHQ)
- Professor Kathleen Richardson, Director of the Campaign against Sex Robots and Professor of Ethics and Culture of Robots and AI at De Montfort University, Leicester
- Warwickshire Police
- Dr Mohamed Khamis, Associate Professor in the School of Computing Science at the University of Glasgow
- Michael Sheath, independent consultant
- The Lucy Faithfull Foundation
- Professor Emma Barrett, Professor of Psychology, Security & Trust at the University of Manchester
- Karl Hopwood from the Insafe network of Safer Internet Centres
- Eveshnie Reddy, Lecturer & Researcher, at the University of South Africa
- Dr Martina Gillen, Senior Lecturer in Law, UWE Bristol

Safeguarding

Safeguarding of children observed during the study

This study did not include any child participants. In circumstances where the researchers have received information that may give cause for concern about a child's safety or welfare, the NSPCC's safeguarding and child protection procedures have been followed. For more information about the NSPCC's safeguarding procedure, please email emergingtech@nspcc.org.uk

If you have concerns about a child, please contact the NSPCC Helpline on 0808 800 5000. For practical advice on safeguarding children using VR headsets, please see the NSPCC's guide: www.nspcc.org.uk/about-us/news-opinion/2022/christmas-vr-safety-advice-for-parents-metaverse

For more resources and guidance on safeguarding children, please see: https://learning.nspcc.org.uk/safeguarding-child-protection

Safeguarding of researchers

Proactive steps were taken to support and facilitate safe and ethical research in adherence with the NSPCC's research ethics policy. Our policy is based on the ESRC Framework for Research Ethics (FRE) and the Government Social Research Unit (GSRU) professional guidance. For further information on the NSPCC's research ethics principles, please see: https://learning.nspcc.org.uk/media/3091/nspcc-research-ethics-principles.pdf

Proactive measures were also taken by Limina Immersive to ensure the wellbeing of their researchers. Topics were assigned to researchers depending on their experience, comfort level and prior subject expertise, meaning that research that had the potential to be more distressing was assigned to the most experienced and trained members of the team. The lead researcher who took on the research topics with the most potential for distress had been specifically trained in techniques for dealing with the process of gathering information that could be upsetting. Management ensured regular communication with researchers continuously throughout the research process, which included wellbeing checks and proactively discussing any mental health needs.

Glossary

360 video: video recordings where a view of every direction is recorded, used in immersive technology.

AI face transfer technology: AI technology that takes a dataset of photographs of a person, often a celebrity, and generates that person's face on the 3D model. This is sometimes known as 'deepfaking'.

Autobiographical memory: memories of significant personal events and experiences in an individual's life are considered autobiographical memories.

Avatar: a character that the user inhabits in VR and AR spaces. An avatar can represent a user in real life or be a persona. Users sometimes build a backstory for persona avatars. They are usually highly customisable.

Avatar commission: getting a personalised, bespoke avatar designed and produced to use in VR spaces. This commission often involves a payment.

Avatar transference: avatar transference, sometimes referred to as mind or consciousness transfer, is a concept in which a person's mind, consciousness, or personality is transferred from their physical body into a digital or artificial one, such as an avatar in a virtual world, a robotic body, or even another biological body. In practical terms, when using a consumer VR headset, avatar transference is often where a VR avatar temporarily feels as real to a user as their own body.

Body disassociation: the experience of not feeling connected to your own body, and/or to perceive the physical world around you as not real.

Camming: performing on a webcam or other streaming device to a live, online audience.

COM-B behaviour model:[4] a model widely used to identify what needs to change in order for a behaviour change intervention to be effective. It identifies three factors that need to be present for any behaviour to occur: capability, opportunity and motivation.

Cultural relativism: the idea that certain beliefs, moral attitudes and practices should be understood only in relation to the culture that practice originates from.

Doxxing: to publicly share a person's contact details including address without their consent.

Eroge games: a visual dating game often involving graphic depictions of sexual activity.

Erotic role play (ERP): refers to the act of users engaging in sexually-themed or suggestive interactions while assuming the roles of their chosen avatars within a virtual environment. It can involve various scenarios, characters, and themes.

Full body tracking kit: technology that can mirror your real-world movements, simulate the sensation of physical touch, and blur the line between 'virtual' and 'real'.

Haptic technology: the use of tactile sensations to stimulate the sense of touch in a user experience, such as vibration in games console controllers.

Hentai: a type of pornography that is anime in style.

Interoperability: the ability of different systems, devices, or software applications to communicate, share, and work with each other effectively.

Live action role play: games that take place offline where players adopt fictional characters.

Lolis: Offender language for avatars designed to look like girls, roughly aged under 16 years.

Offender disinhibition: disinhibition is the state when people feel able to transgress social norms; in the case of VR offenders, it is when they feel safe to commit offences they may otherwise feel restrained from committing.

Online role play: online games based on storytelling where players take on fictional characters.

Parasocial relationship: a parasocial relationship is a psychological attachment or connection that an individual forms with a media figure, such as a celebrity, influencer, or fictional character. These relationships develop as a result of consuming media content.

Phantom touch: the psychological feeling of touch in VR whereby the brain 'fills in the gaps' and believes the person is experiencing physical touch.

Proprioceptive drift: a phenomenon often observed in experiments involving the rubber hand illusion, a well-known psychological experiment that investigates body perception and the integration of multisensory information. In this illusion, participants are asked to place one of their hands out of sight while a fake rubber hand is placed in their field of view. The experimenter then simultaneously strokes or touches both the real and the rubber hand. As a result of this multisensory stimulation, participants often begin to feel as if the rubber hand is part of their body and start to experience the sensation of touch on the fake hand. Proprioceptive drift refers to the shift in the perceived location of the participant's real hand towards the position of the rubber hand.

Sandbox game and VR sex sandbox game: a sandbox game refers to a type of video game that provides players with an open-world environment where they can freely explore, create, and interact with the virtual world and its elements without being restricted by a linear narrative or specific objectives. VR sex sandbox games provide a set of tools for creating and animating sexual scenes, designing custom environments, and scripting interactions between characters.

Scalability: the capacity for a technology platform to grow its user base, sometimes very fast.

Sideloading: the process of transferring files between two local devices, in particular between a personal computer and a mobile device, such as a mobile phone, smartphone, PDA, tablet, or e-reader. Often these sideloaded apps are unapproved or from an unapproved retailer.

Virtual assault: also known as 'assault in VR' or 'simulated assault' describes a physical, threatening and unwanted interaction between two or more avatars that does not carry any legal weight.

VR early adopters: people who started using VR technology before it went mainstream.

VR exposure therapy: a form of psychotherapy that uses virtual reality technology to help individuals confront and overcome their fears or anxieties in a safe and controlled environment. It is a type of exposure therapy, a well-established psychological treatment method, in which patients are gradually exposed to anxiety-provoking stimuli to reduce their fear response over time.

Foreword from the CEO

"Technology companies that are building the next frontier of communication tools must learn the lessons of the last 20 years – children's safety must be built into the design and infrastructure of their platforms.

Children cannot be an afterthought."

Last year, I used a virtual reality headset for the first time and stumbled across two avatars playing basketball in the metaverse. I was thrown a virtual ball and decided to take a few shots.

You may think that there is nothing unordinary about three people playing basketball together. But after one of the avatars spoke, I realised that these were two children, I would guess between 9 and 12 years – significantly below the 18+ age rating – and after speaking with them, I realised that these boys did not know each other in real life. They had met in a virtual chat room and one claimed to be using his parent's account to play from his own bedroom.

What struck me was how lifelike the experience seemed and the ease in which children and adults are able to connect and engage with each other in these spaces. While this encounter was an innocent one, I was concerned by how unsupervised and vulnerable they were in this environment. Afterwards, I became curious to know more about what children might be coming across when using this technology.

In recent years, immersive technology has harnessed our imagination and opened a whole new world of experiences. For children, virtual reality has created new ways of learning about the world and fashioned a user-centred environment for sharing information, playing games, and having new experiences with peers.

It is our duty to ensure that we understand everything we can about this new digital landscape so we can protect the youngest and most at risk in our society.

We commissioned this important research to both explore whether this new technology is already causing harm to young people and to ascertain the future harms we can expect as this technology evolves.

I would like to thank Limina Immersive for undertaking this research on our behalf. I am deeply concerned by the evidence of child sexual abuse that this project has uncovered. It is clear that the risks children are experiencing when using immersive technology are no longer on the horizon. They are happening now.

The digital world can be both a playground and a battleground. While it offers innovative ways for our children to connect, learn and grow, emerging technologies also present a new range of risks to children's safety online.

Emerging data tells us that the isolating nature of VR headsets alongside a lack of regulation produces an environment where online sex offenders can exploit children with ease.

Likewise, the anonymity provided to users increases the risk of harm taking place. VR spaces now offer a place where offenders can act out illegal behaviours without any form of accountability and children can be left isolated when dealing with the harm they experience, without adequate support.

However, we must find hope that there is still a window of opportunity. Immersive technologies are still being developed and rolled out to young people and there is time for technology companies to take responsibility to ensure that their devices are created with safety in mind. Technology companies that are building the next frontier of communication tools must learn the lessons of the last 20 years – children's safety must be built into the design and infrastructure of their platforms. Children cannot be an afterthought.

During my 10 years at the NSPCC, I have continuously campaigned to make the online world safe for children. However, cyberbullying, online grooming, exposure to harmful content, and now, the increasingly blurred boundaries between the digital world and real-world experiences, all continue to pose a substantial safeguarding risk to children.

As the Online Safety Bill completes its passage through Parliament, this paper shows how important it is that new and emerging technology is within scope of the legislation.

The new online safety regulatory regime needs to be future-proofed, so children are protected from new and emerging harms. One way this can be achieved is through the regulator, Ofcom, engaging with and listening to the voices and experience of children.

We must ensure that our children can enjoy the benefits of immersive technology safely. This will involve necessary cross-sector collaboration, including educators, parents, policymakers, and the technology industry.

The findings from this paper should act as a wakeup call to us all. Now is the time to unite our efforts and work collectively towards creating an online environment that is as safe as it is innovative.

Thank you,

Peter Wanless
Chief Executive Officer
NSPCC

NSPCC

Foreword from the NCA

"These are new, more technically complex and rapidly evolving immersive spaces which - due to their nature - have the potential to exacerbate online abuse, unless they are designed to effectively protect children."

Every year the NCA publishes its National Strategic Assessment, which covers the scale, complexity and severity of Serious Organised Crime (SOC) threats. Over the last few years we have developed new methodology which estimates that there are between 680,000 and 830,000 UK-based adults who pose varying degrees of sexual risk to children; this equates to 1.3%-1.6% of the adult population. The Independent Inquiry into Child Sexual Abuse found that one in six girls and one in 20 boys will have experienced sexual abuse before the age of 16, but only one in six victims will report it. These are extraordinary figures and reflect a better understanding of a harm that has historically been underestimated, and continues to be under-reported. This increase is likely caused in part by the radicalising effect of internet technologies: the widespread availability of videos and images of children being abused, and groups sharing and discussing the images online, has normalised such behaviours. Offenders also seek out online spaces which children use, where they initiate contact, groom and abuse them, and seek to meet them offline. A lack of effective protection and security measures by platforms allows this to happen. Only a whole of society response can begin to address the scale and impact of this threat.

It is in this context that we welcome the NSPCC's work to understand and publicise the growing and changing threat to children from the extended and virtual reality (VR) technology. These are new, more technically complex and rapidly evolving immersive spaces which - due to their nature - have the potential to exacerbate online abuse, unless they are designed to effectively protect children.

Whilst offending within the wider extended reality sphere is currently relatively low in volume compared to traditional online CSA offending, we anticipate this is likely to increase over the coming years as the availability and popularity of VR and Augmented Realities (AR) technologies increases. We and our partners have a range of concerns including the creation and use of child sex abuse material (CSAM) within these new environments, and the customising of technologies such as haptic interactions, which may be lawful in the adult sex industry, to enable extreme or indecent criminal acts including targeting children.

In our view it is critical that companies which are providing and shaping these environments pay attention to self-regulation and the development of appropriate safety systems; the Government's Online Safety Bill would ensure that in-scope companies providing extended reality services to UK users assess the risks on their services and put in place mitigations, including where appropriate reporting to law enforcement.

The NCA is committed to tackling child sexual abuse in the online, virtual and physical environments. We work closely with a wide range of partners in the UK and overseas to monitor offender take-up of new and emerging technologies and to bolster our collective response. We will continue to identify, investigate, and disrupt offenders using immersive technologies, including bringing offenders to justice where we can. Equally importantly, we will continue to work with partners, including the NSPCC, to protect children and young people from online sexual abuse through our education outputs. We provide advice, guidance and resources for children and young people, the professionals who work with them, and their parents and carers through our CEOP Education products (CEOP Education). The NCA also continues to support the work of the NSPCC and other partners in highlighting risks to children and we will continue to review our response so that

we adapt to the ever-changing technological landscape.

We would like to thank the NSPCC and the authors for this work, which shines a spotlight on the growing risks posed to children in extended reality spaces. Law enforcement, governments, technology companies, and all relevant stakeholders must act robustly and with foresight to ensure online safety for children and other vulnerable members of our society. A combined effort is needed to ensure that effective safety systems and processes are built into emerging technologies from their inception.

Immersive technologies are hugely powerful. This is the moment for collaborative work to ensure that they are a positive force in our children's lives and we have done everything reasonably possible to make them a safe space to explore and enjoy. We believe law enforcement, industry and government need to collaborate dynamically to ensure we can understand and address these issues. We call on all immersive technology companies to urgently review the risks on their platforms, be transparent about what they find, and take the necessary mitigation steps. We will continue to support and work collaboratively with all partners to protect children and vulnerable people and bring offenders to justice.

James Babbage
Director General Threats
National Crime Agency

NCA
National Crime Agency

Foreword from Limina Immersive

"The risks are real and present, and it is incumbent on us to act swiftly to address these dangers. Luckily, significant change is still possible, as this form of digital media is relatively new and therefore still malleable."

As we stand on the cusp of a new era of technological advancements, it is our collective responsibility to ensure that these tools are used for progress, and not harm. The papers that Verity McIntosh and I have each authored are a sobering testament to the potential risks and harms that virtual reality (VR) and augmented reality (AR) could pose to children if left unchecked.

Immersive technologies, such as VR and AR, offer a world of opportunity; the scope of which we are only just beginning to comprehend. However, the same technologies present an equally potent risk, particularly when it comes to the safety of our most vulnerable citizens – children. The risks are real and present, and it is incumbent on us to act swiftly to address these dangers. Luckily, significant change is still possible, as this form of digital media is relatively new and therefore still malleable. The technology landscape is in flux, and it is in this state of flux that we have the chance to implement necessary changes and set a precedent for future developments in the field of immersive technologies.

The evidence provided in this paper serves to underline the profoundly distressing potential of immersive technology to be used as a tool for child sexual abuse (CSA) and child sexual exploitation (CSE). This extends to both online and offline offending, with perpetrators utilising the anonymity provided by these technologies to groom and exploit children. We are also presented with the chilling reality that these spaces are being used to simulate sexual abuse with 3D models of children, a gross violation that normalises abusive behaviour and carries the risk of leading to contact offending.

Some findings may be shocking, but this paper is not intended to induce fear or discourage the use of immersive technologies. On the contrary, it is about improving the safety of these technologies and implementing robust protections for children. The positive potential of VR and AR cannot be fully realised without trust, and trust cannot exist without safety.

I am so grateful to my corresponding author, Verity McIntosh, who authored the first paper in this two-part series, and who has worked with me for several years in this field, bringing her tenacity and deep insights to the issue. I owe a debt of gratitude to our dedicated researchers who assisted in the research; Emma Hughes and Joanna Henderson, who carried out multidisciplinary research with painstaking attention to detail. I am also deeply grateful to our editor, Sian Norris, whose work has been crucial in ensuring the clarity, coherence, and overall quality of these documents.

I want to thank the NSPCC. Their unwavering support and commitment to the protection and welfare of children cannot be overstated – both online and offline. As the commissioner of this project, their drive to safeguard the wellbeing of children has underpinned every stage of this endeavour.

Finally, we owe immense gratitude to the Oak Foundation. Their financial support has been crucial in bringing this project to life.

It is thanks to The Oak Foundation and the NSPCC, such forward-thinking organisations, that we are able to undertake such vital work.

Catherine Allen
CEO and lead consultant
Limina Immersive

LIMINA IMMERSIVE

Executive summary

Emerging technologies bring incredible opportunity. They also come with risks, particularly to child safety. Immersive technology is no exception.

This paper reveals how immersive technology, such as virtual reality (VR) and augmented reality (AR), is putting children at risk of child sexual abuse (CSA). These risks are present, with harms being enacted on children in VR spaces by offenders at the time of writing. At the same time, the risks are evolving, with offenders finding new ways to exploit immersive technology to groom, coerce, sexually abuse and exploit children.

Abuse can happen solely within a VR space. It can also lead to offline 'real life' offending, with perpetrators using VR spaces to interact with and gain the trust of children in order to arrange meet-ups and engage in CSA and child sexual exploitation (CSE).

The research also evidences how immersive technology is allowing offenders to simulate sex with 3D models of children, including those modelled to look like children they know 'in real life'. The risks are that this could both normalise abusive behaviour and potentially lead to contact offending.

The threats to children are real and present. But the closed nature of many VR communities means it can be difficult for people involved in these spaces to speak out. The research found, through secondary sources, individuals saying that they tried to raise the alarm about sexual abuse or harassment within multi-user VR spaces, and in response had been subject to retaliatory threats, including of having their personal details revealed online. For children, the known barriers to reporting sexual abuse that exist offline also exist within VR spaces. Research by Manay & Collin-Vézina (2021)[5] found that up to 52 per cent of children have remained silent about the sexual abuse they have experienced. Through secondary sources, we have observed that additional deterrents from reporting CSA in VR are fears of exacerbating the violence, and because children are worried their parents will ban them from using VR.

The research also explored the broader issues of depersonalisation and disassociation in VR. Users can often experience a disassociated feeling when leaving an immersive space: the feeling that the world around them is not real.[6] Victims of CSA and CSE have also been known to disassociate from their body as part of a trauma response. Therefore, there could potentially be a heightened risk of a disassociation when a child suffers sexual abuse in a VR space.

The research found that offenders also experience this disassociation. This finding has led the authors to posit that this could lead offenders to a long-term build-up effect where the constant body transference into the simulation of a person committing heinous acts creates a bodily association with that character. This could risk the offences escalating into offline offending.

The paper notes that how children's data is used in VR is a key issue in terms of safeguarding. Data privacy can be a double-edged sword. It can help to encourage child safeguarding and reduce the risk of abuse and exploitation, particularly the risks of an offender accessing a child's location and contact details; or the risk of an offender accessing images of a known child in order to use that to create a child model for sexual gratification. However, data encryption can also pose risks: protecting offenders' identities and hiding abusive content.

Despite the evidence for risks to children posed by immersive technology, and their predictability, there is also substantial evidence to show that tech companies failed to prioritise child safeguarding when designing their platforms.

This was particular apparent in the lack of parental control when a child is using VR. It is important to note that unlike in 2D internet, or on a gaming console, a parent cannot simply look over their child's shoulder and view the material they are watching or interacting with. Instead, a child is in a 3D world that only they can see and interact with.

The newness of VR and its association with futuristic, almost sci-fi visions, means that parents and carers who are not highly tech literate may not understand what VR is or looks like. They may assume it is a game or a cartoon and does not pose a threat to their child. This lack of immersive literacy and understanding in the general public gives offenders more leeway to abuse, free from much scrutiny and accountability.

The NSPCC has developed recommendations with support from Limina Immersive for government, the regulator, law enforcement bodies, and the technology sector based on this research. There is no reason why change cannot happen now to create a safer immersive technology space. VR and AR also bring positive opportunity to society, but this cannot be realised without safety and trust.

The technology is still new, evolving and malleable. Government, civil service, tech companies and law enforcement can all play a vital role in safeguarding children and limiting the online harms immersive technology can bring.

Recommendations

UK government

- Review legislation on a rolling basis to ensure that immersive environments are adequately covered
- Consider whether there is a case for creating new offences for simulated abuse
- Ensure that child safety is factored into all policy making related to emerging technologies
- Build an understanding of immersive technologies amongst decision makers and safeguarding professionals
- Provide more guidance, funding and learning opportunities to local law enforcement for how to appropriately respond to simulated offences, including those in VR

UK regulators

- Ofcom should engage with immersive technologies as a distinct form of media
  - Focus on balancing privacy and security concerns for age assurance and safety in immersive environments
  - Understand how threat is different in immersive environments
  - Produce a regulator 'state of the nation' report on emerging technology risk
- Ofcom should respond to the risks of immersive environments in regulation
  - Develop clear guidance on how immersive technology platforms should assess and respond to risks
  - Issue a dedicated code of practice on immersive environments and third-party VR apps
  - Issue specific guidance on tackling cross-platform risk
  - Provide clear age assurance guidance
- Ofcom to consider the role that VP app stores can play in keeping children safe

UK law enforcement

- Increased dialogue between civil society and law enforcement
- Increased engagement on the metaverse

Technology sector

- Implement safety-by-design across all VR and AR products
- Foster a proactive approach to child safeguarding in immersive environments
- Transparency in the reporting and moderation process
- Include easy to use parental supervision co-location features and improve parental education
- More data needs to be made available to civil society

Introduction

Virtual reality (VR) and augmented reality (AR) is on the rise in the UK. According to our 2021 tracker, which surveyed 1,500 people between January 2021 and December 2021, the proportion of UK adults who have experienced virtual reality more than doubled, from 10 per cent to 22 per cent.[7]

Virtual reality places users in the centre of a 3D environment where they are completely surrounded, in order to experience the sights and sounds of a simulated scenario. Augmented reality preserves the user's view of the physical world, adding digital objects and adaptations to give a blended view of the physical and digital surroundings. For further information on VR and AR technology, please see our supplementary paper *Child Safeguarding & Immersive Technologies: Key Concepts*

Every year, some of the world's largest and most valuable companies invest billions of dollars[8] into immersive technologies. The invested amounts are the equivalent to many countries' GDPs. We view these companies to have similar goals, with the aim to have immersive technologies become commonplace in our everyday tech life, just as social media has become.

Immersive technology is increasingly becoming a part of many children's lives and continues to grow in prevalence. According to Common Sense Media's 2021 survey,[9] 27 per cent of young people aged 13–18 years and 22 per cent of children aged 8–12 years have experienced VR in the US.*

However, it should be noted that, at the time of writing, the majority of VR headsets impose a lower age limit of 12 or 13 years of age.[10]

There are a range of activities that children currently take part in through VR without issue, including exercise games and family challenges. We believe VR has the potential to be a fantastic educational and social research tool for children and young people. It can encourage children to develop empathy, help them explore the world around them, and promote fitness.

Research undertaken for this paper has found, however, that some particularly popular VR spaces and platforms are not prioritising children's safety, resulting in harms taking place right now, including child sexual abuse (CSA) and child sexual exploitation (CSE).†

The risk to children is present and happening within, or because of, VR. This paper outlines and categorises those present risks, as well as the likely future risks that children face, with analysis and guidance on how these pressing issues can be tackled by policymakers, regulators, law enforcement, and the technology industry.

In our view, risks to children through immersive technologies are currently much more present in VR than AR. Based on the evidence available in the current landscape, this paper will primarily cover harms we have identified in VR. However, we believe this is likely to change in the future as AR headsets become more widespread. The research also indicates that offenders' use of certain VR simulation content can put children at risk, due to how certain platforms normalise child sexual abuse, and allow users to simulate child sexual abuse. This can lead to offline offending against a child who may never have tried VR.

To us, it does not matter if you have never put on a VR headset: these threats concern all of society.

While the paper findings are concerning, if policymakers, law enforcement, and tech companies act now, they can respond to these risks and ensure children are better protected. Action must be taken to pre-empt evolving risks, making VR a safe and welcoming space for all. Technology companies are making decisions every day about the design and

* According to the Institute of Engineering Technology (IET) 2023 study of UK parents, with children under the age of 13, 25 per cent of children aged between five and 10 years use VR weekly. Institute of Engineering Technology (2023), *Pixels overtake playgrounds for kids' social lives*. Accessed 12/07/2023 on www.theiet.org/media/press-releases/press-releases-2023/press-releases-2023-april-june/8-june-2023-pixels-overtake-playgrounds-for-kids-social-lives/

† The NSPCC views child sexual exploitation (CSE) as a type of sexual abuse. However, this paper will refer to CSE as a distinct category to reflect how it is classified in the UK's Online Safety Bill and Sexual Offences Act 2003 as child sexual exploitation and abuse.

build of their software and devices. Here, there is an opportunity for necessary change. Our paper aims to constructively support the sector by identifying safeguarding gaps and blind spots, with a focus on ensuring that platforms have a proactive safety-by-design approach.

For many, notions such as 'the metaverse' and 'virtual reality' have felt like concepts that belong in the realms of science fiction and futurism. These futuristic assumptions might result in trivialisation and even sometimes a refusal to engage. By laying out the very real risks that children face, we hope this paper demonstrates the urgency for policymakers to critically engage with immersive media. There is a vital window of opportunity to legislate for and regulate this form of media while norms are still being shaped. The incoming online safety regulatory regime will create new incentives for tech platforms to change their behaviour.

This paper does not suggest that children should be prohibited from VR or to say that children using VR is wholly problematic. It is the view of the NSPCC and Limina that children above the VR headset's lower age limit should be able to use VR age-appropriately, safely, and without fear of abuse. That is why it is essential that platforms are designed with safety in mind.

Methodology

The project utilised a range of methods to gather insight on the CSA and CSE risks to children in VR and the metaverse. These methods included interviews, focus groups, a literature review, primary data collection and additional desk-based research.

Interviews and focus groups

A total of 11 in-depth interviews were conducted with professionals who have expertise in emerging technologies that may pose risks to children. Participants included academics, UK civil service officials, representatives from UK law enforcement agencies and UK and EU civil society organisations, as well as independent experts in the field of emerging technology risks and child safeguarding. Interviews were conducted between August and October 2022. The researchers also conducted two focus groups with professionals from regional law enforcement, and in-depth interviews with professionals from the UK national policing Online Child sexual abuse and exploitation Covert Intelligence Team (OCCIT). These discussions offered vital insights on present knowledge, as well as understanding of the anticipated threats and harms from VR.

Light-touch literature review

A non-systematic review of studies about risks to users of virtual reality was conducted on an internet search engine, using the base search terms 'VR', 'virtual reality', 'virtual worlds' and 'augmented reality'. The studies identified through this approach included ethnographic research, academic reports, expert interviews in newspapers articles, and investigative documentaries. Additional studies recommended by interview participants were also reviewed. The reviewed materials were used to build an understanding of the current risk landscape.

Primary data collection

Between June and November 2022, the researchers visited popular virtual reality platforms to observe their environment and interactions between users. The main purpose of these sessions was to confirm the phenomena cited in the literature and signposted to by interview participants. The number of visits and duration of sessions was determined iteratively, and visits were repeated or extended when observations made in initial sessions raised additional questions that required further exploration. The researchers identified those they believed to be child users on these sites through voice and body language (no additional validation process was used).

Other desk-based research

Between June and October 2022, the researchers conducted the following:

- a non-systematic scan of user reviews of VR platforms on app stores
- a non-systematic review of major marketing materials for each major VR platform, including promotional material on app stores, the company website, and membership platform page
- a scan of the Terms and Conditions of popular immersive technology products and platforms, with a re-review of the Terms and Conditions in March 2023.

Since these activities were not undertaken systematically, findings from these sources may not be fully representative of user views and marketing materials, and do not offer a comprehensive assessment of Terms and Conditions of these products. It should be noted that motivations for submitting user reviews may vary, and the reviews encountered during our scanning exercise may not reflect true user experiences.

Limitations in methodology

No data collection was carried out with child users of VR technologies. Moreover, the literature review did not identify any systematic data (e.g. from user surveys, diaries, or ethnographic observation) that could provide insight into children's views and experiences of using VR. While we are aware of popular online forums containing users' first-hand reports of their experiences in VR, we have not relied on these for information; this is because it was not feasible to secure informed consent from users to use their posts for research purposes. This research therefore relies on deducing children's experiences and the risks they face through the views and observations of the expert authors, researchers and experts who participated in interviews and focus groups. The secondary nature of the authors' sources should be taken into account by the reader.

The harms

This chapter outlines the sexual risks that children face in VR environments. The evidence base for harms is fragmentary – as we would expect from a technology whose adoption is still limited. The sections below piece together this evidence to provide a comprehensive picture of what is known to date about the risk landscape for children in VR.

Children's presence in VR multi-user spaces

There is no definitive data on the extent to which children use VR spaces, and the number who would therefore be exposed to the risks outlined below. Currently, there is little data on user demographics of the most popular multi-user VR online platforms. Platforms do not often share sales and usage data, and there are no legal mechanisms in place to compel them to publish it. It is vital that technology companies publicly share more data on children and other users' presence in VR in order for researchers and civil society to conduct thorough assessments of children's safety in VR.

Survey figures on headset ownership indicate that at least a proportion of children have access to VR spaces. According to a survey by the research agency Morning Consult for Piper Sandler, 26 per cent of US teenagers own a VR headset.[11] Equivalent figures are unavailable for the UK, and these challenges will persist while there is limited data transparency, but we expect figures would likely be lower as only six per cent of UK adults report having a VR headset in their household.[12]

Regardless of headset ownership, we can be confident that children do visit such spaces. Research by Common Sense suggests that 27 per cent of 13–18-year-olds in the US "have ever used virtual reality", with 3 per cent using it every day and 9 per cent at least once a week.[13] Field research from a previous project conducted by Limina Immersive found children in VR spaces, with many being below the lower headset age limit of 13 years.[14] Experiences of UK law enforcement officers in VR echo this observation:

> *"Our operations and research shows that the demographic includes many users who are very young – younger than 13..."* (Specialist UK law enforcement officer)

Children's presence in VR environments was also observed in research by US non-profit SumofUs[15] and research by the Center for Countering Digital Hate[16] while numerous reviews on VR app store platforms and elsewhere describe, and indeed often complain about, just how many children there are in these spaces.[17]

The above suggests that a sizeable minority of children using VR spaces are exposed to the possibility of harm and may, therefore, be considered to be at risk today.

However, the numbers who have actually encountered these risks is much harder to estimate. We are not aware of any research with children that explores their experiences of harm in VR spaces. While research does exist where researchers have observed and recorded harmful incidents to children in VR environments,[18] it is not possible to extrapolate the proportion of children who have so far been harmed. Calculations are also complicated by the fact that children are not easily recognisable in these spaces, as their chosen avatars may not reflect their true identity; and are further confused by adult users who adopt child-like avatars or pose as children.

The sections below do not attempt to enumerate the frequency of harms to children; instead, they describe the nature of the harms. We provide evidence of instances where harm has occurred or, where this is unavailable, the rationale as to why we believe harm is likely to be happening or is anticipated in the near future.

Sexual grooming in VR multi-user spaces

"There's a massive grooming problem in multi-user VR platforms, a lot of grooming situations: paedophiles, dating age gaps...people lying about their ages." (User sharing her experiences through a video on a popular social media platform, paraphrased to protect anonymity)

"[The] metaverse connects users not just to each other but to an array of predators, exposing them to potentially harmful content every seven minutes on average. If the metaverse is safe for predators, it's unsafe for users, especially children."[19] (Imran Ahmed, Chief Executive of the Center for Countering Digital Hate)

Definition

Online grooming or solicitation is defined as the deliberate establishment of an "emotional connection and trust with a child, with the aim of engaging them in sexual behaviour or exploitation using technology".[20]

Grooming is a risk on a range of online platforms where users who may not have a pre-existing offline relationship have the opportunity to spend time together online.[21] Evidence suggests that online child grooming has increased dramatically in recent years, and especially during the COVID-19 pandemic and associated lockdowns.[22] The NSPCC's Freedom of Information figures indicate that there were at least 6,156 'sexual communication with a child' offences in the UK as of 2021/2022. According to the NSPCC's figure, these offences have increased by more than 80 per cent since 2017/18.[23] In England and Wales, obscene publication offences against children rose sharply in 2013/14[24] and have since shown similar annual increases.[25] The NSPCC found over 30,000 obscene publication offences against children were recorded by police in England and Wales in 2021/2022.[26]

While the risk of online grooming is proven on popular social media channels, we believe it also applies to VR multi-user spaces. In theory, there are various ways offenders could exploit interactions in VR multi-user spaces to groom and solicit children.[27] Offenders can start a conversation in the VR space and build up a trusting relationship with a child. Where users inhabit an avatar that conceals their real identity, a child may have no idea they are interacting with an adult. Unlike 2D social media platforms, there can be the illusion of getting to know someone physically and building a rapport, involving gesture and body language. As this relationship builds, a child may have every reason to believe they are interacting with a peer. This is a clear risk and an obvious example of platforms failing to consider child safeguarding in their design.

Evidence of this risk

There are several known instances of VR grooming leading to offline offences. US police reports and media show how a 33-year-old man in Florida had been living secretly in a teenage girl's bedroom for over a month. He had met and groomed the victim on a popular multi-user VR space, and the victim referred to the abuser as her "boyfriend".[28] The testimony of Maze Marlow, a regular VR user and whistleblower who spoke to BBC reporter Angus Crawford in a 2022 BBC investigation, offers other examples in which digital harm can escalate into real life assault, as well as repercussions to those who raise the alarm about criminal sexual activity in these spaces.

Abuse and harm can also exist *within* the VR space itself. It does not rely on an offender arranging to meet a child offline. VR multi-user spaces provide opportunities for offenders to commit child sexual abuse against a child **in virtual reality** and engage the child in child sexual exploitation **in virtual reality**.

One mechanism for this is through the use of erotic role play (ERP). Angus Crawford's BBC investigation[29] reported witness testimony of children being groomed in multi-user VR spaces. A whistleblower who took part in the programme gave an example of a teenage child who had been groomed and coerced into a private 'erotic role play world', designed like an underground dungeon, by an adult man. The offender preyed on the child's lack of awareness about the technology underpinning these multi-user VR spaces. The child was sexually assaulted by several adults within the VR space. The offenders were all aware they were abusing a child. The abuse continued, with the child repeatedly groomed and coerced into taking part in ERP with adult users. The child did not tell their parents about what happened as they feared they would not be allowed to use VR anymore.

Another mechanism for grooming and exploitation is through VR strip clubs, where children can be manipulated into performing dances for viewers in exchange for money. There is early evidence to indicate that children may already be being exploited in VR strip clubs;[30] however, there is not yet enough data to determine the scale of this activity. Please see the later CSE section in this paper for further detail.

Investigations by documentary filmmaker BrandonFM includes VR users alleging prolific levels of grooming occurring within VR spaces, with offenders consistently grooming, coercing and sexually assaulting children in popular platforms, at scale. Testimony from victims reveals the organised and cult-like dynamics of certain offenders who will use a combination of 2D platforms and multi-user VR spaces to communicate with victims and commit their crimes. One victim, who wished to remain anonymous described their experiences:

> *"[The offender] groomed me and has [also] had sexual experiences with a lot of my friends who are also under 18 years old. The mental scars that this whole experience has put on my mind are so extreme that I was recently diagnosed with Stockholm Syndrome...it was so normal for [the offender] to have relationships with minors, in the bubble that we lived in...I came out of that situation with severe trust issues, and I am not sure when things will go back to normal."*[31]

The described offender 'helped' victims cultivate 'phantom touch', which then formed a part of later assault in VR.

What do we know about grooming offenders in VR environments?

There is a body of evidence on the characteristics of people who groom children online,[32] but little is known about offenders operating in VR spaces. The University of Manchester's report *The Future of eXtended Reality Technologies, and Implications for Online Child Sexual Exploitation and Abuse* notes that studies show "the prototypical online offender is most likely to be male, Caucasian, single, aged in their 20s or 30s, with higher academic and occupational ability, low in antisocial traits, showing good functioning in society, but with demonstrable sexual deviancy".[33] It is worth noting that there is particular crossover between these demographic traits and the demographic skew of VR early adopters.[34]

Interviews with law enforcement professionals indicate that offenders look for places to groom children online where

a) there are many children and opportunities to offend, and
b) there is a low chance of repercussion.

VR multi-user spaces currently fit the profile for a "target rich environment",[35] where offenders can potentially act out harmful or criminal behaviours with little in the way of sanction or moderation. One user who reviewed a leading platform after spending 78 hours on the app said it was "a cesspit full of paedophiles [sic]".[36]

UK law enforcement representatives also confirmed in interviews that CSA offenders are now holding meet-ups with other offenders on a leading multi-user VR platform.

The extent to which these risks are new

- **A sense of physical presence combined with anonymity**

  The physical presence and intimacy that VR allows for, mixed with online anonymity, is a unique combination that we believe offenders may exploit to manipulate children. Unlike 2D platforms, anonymity or disguise can be combined with gesture, movement, voice communication, facial expression, and body language, all of which can potentially enhance the offenders' capabilities to create intimacy and rapport with a child.

- **Atmosphere**

  In our experience, VR environments sometimes carry a sexual 'atmosphere' or 'vibe'. We believe that offenders can exploit this atmosphere to disinhibit and normalise sexualised behaviours and coerce children into sexualised activity. They may for example take a child to a virtual strip club, dungeon or sex toy room. This is akin to how a contact offender might take a child to a nightclub or house party as part of their grooming process. It is important to note that if an offender took a child to a city centre commercial strip club, it would likely be noticed and, hopefully reported. But the nature of VR means that certain activities can happen out of sight or unremarked, or children can be brought to VR spaces that are dedicated to offending.

Design characteristics that contribute to this harm

- **Lower age limits for some platforms are not communicated clearly in the VR app stores or marketing material**

  In our review of marketing materials, lower age limits are usually in the small print, potentially making it unclear to parents that the activity is designed for adults. This likely contributes to the high proportion of children reported by other users in these particular multi-user VR worlds.

  In researching this paper, multiple government and third sector agencies raised concerns about the apparent abundance of children gaining easy access to (notionally) age-controlled platforms, and of adults gaining easy access to children.

- **Most multi-user games in VR have an animated, 'cartoony' aesthetic that can appear childlike**

  In our review of activities on numerous platforms, we found that many activities had the appearance and feel of children's games – although they are not. Some include childlike aesthetics, but activities that are not age appropriate for children. We believe this can cause confusion for both parents and children, who may assume that these childlike activities are safe and appropriate. This suggests that children are at risk of being exposed to adult behaviours that are not age appropriate.

- **Avatars are not connected in any way to a person's real-life identity**

  Arguably, one of the major attractions of VR metaverse spaces to many users is the fact the space allows its users to experiment with different identities. A marketing message surrounding the 'metaverse' that has cut through to the general population is that it is "a virtual world where you can be anyone and do anything you want".[37]

  However, this poses two issues. The first is that there is very little real-life identity checking in VR spaces. This means offenders can potentially treat VR worlds as places where they can act with impunity.

  The second is that offenders can select and design avatars chosen to attract children, manipulating them to let their guard down. For instance, a man in a recent *Dispatches* investigation[38] said he "liked girls between nine and 12 years old". He said this while inhabiting a cute, harmless looking ginger cat avatar.[39] A child interacting with this adult in that avatar may assume that he was their peer, with no way of knowing his real age or sex.

- **Terms of service and community guidelines are often written in 2D, plain text within the VR space**

  When reviewing Terms and Conditions for various VR products, we found the formatting of terms of service agreements and behavioural guidelines difficult to read in a VR headset. The text can also feel arbitrary, therefore making it unlikely to serve as much of a deterrent to offenders. The lack of clear deterrent can contribute to a feeling that VR multi-user spaces are a 'wild west' where there are no rules. The offer from VR companies is that users have entered a world where 'anything is possible'. We believe this can have a disinhibiting effect on offenders, exposing children to risk.

Other issues include lack of moderation resource and lack of transparency in the reporting process. These issues are explored in the analysis section of this document.

Sexual harassment and assault in VR multi-user spaces

"She was raped by a user [...] all while another user in the room watched and passed around a vodka bottle." (An account from the NGO SumofUs, where an adult researcher was virtually raped in a VR multi-user world)

Definition

Sexual harassment and assault in VR can be defined as "unwanted, digitally-enacted sexual interactions".[40] One form of sexual violence in VR is 'virtual rape', which specifically refers to "a situation in which a user's avatar is forced/coerced into sexual activity against his/her wish".[41]

Evidence of this risk

Documentary filmmaker BrandonFM has documented numerous accounts of sexual harassment and assault towards children across popular VR platforms.[42] In an interview he conducted, a girl, who wished to remain anonymous described sexual abuse as "common."

> *"You know, you go to the [nightclub venue in multi-user VR platform] and you'll see people hitting on underage girls and they [the girls] are like 'I can't, I am 16', and [the perpetrator] is like 'that's ok, it's just online'. Which is not okay... Since its online, [perpetrators] feel like it doesn't really matter because it's not necessarily real, but the mental effect it has on the minor is real."*

Further evidence of this harm was provided by an undercover BBC reporter who posed as a 13-year-old girl, entered a popular multi-user VR space, and was sexually assaulted.[43] Researchers from the Center for Countering Digital Hate observed a child being followed by two heavily breathing men while in the same platform, with another male joking that one of the men was a "convicted sex offender".[44] One of this paper's co-authors was forced to intervene in a different VR platform when, during field research for another project, a group of men made jokes towards the author and a nearby child about them both being raped by multiple men. The child had previously told the author she was seven years old.

Who is targeted in VR environments?

Research from US research firm The Extended Mind[45] shows that 49 per cent of female regular VR users have experienced sexual harassment in VR, compared with 36 per cent of men. This suggests that sexual harassment and assault in VR may be a gendered form of harm. The same research shows that women perceive it this way, and that fear of sexual harassment is a major barrier for women's use of VR platforms.

While there is no evidence that this sort of sexual harassment offender specifically targets children, it is worth noting that the lack of safeguarding mechanisms in VR spaces, and the failures to implement age limits, means a perpetrator intent on committing sexual assault would not necessarily know the age of the person they are committing the offence against. Without voice cues, it is hard to tell how old someone is by their avatar, as avatar age in VR multi-user worlds does not usually correspond with the actual age of the user. This means that children are – perhaps inadvertently – at risk of online harassment.

The extent to which these risks are new

- **Heightened impact of assault in VR**

  It is often said that the 'metaverse' is when your body 'enters' the internet. Sexual assault in VR is subsequently a full body experience. Phantom touch can mean that victims of VR sexual abuse experience the physical sensation of being touched without their consent, assaulted, abused, and even raped. We believe that the combination of the phantom touch phenomenon, the sense of presence, and the emotional intensity of being in the VR space all combine to heighten the impact of sexual offences to the victim. Victim testimony refers to feeling "dehumanised" and "objectified" for a long time after the assault itself.[46]

- **Offender disinhibition**

  VR is known to have a disinhibiting effect: studies relating to the 'online disinhibition effect'[47] suggest that users have a tendency to perceive cyberspace as a distinct, transitional psychological space,[48] creating an 'anything goes' mentality.

  We believe VR multi-user spaces can provide offenders with both the opportunity to offend, and a sense of disinhibition. This can lead to a greater acceptance of abusive behaviour against children. As with grooming in these spaces, avatar disguise and anonymity may also contribute to a feeling of impunity.

- **Multi-user VR worlds invite the creation of tighter knit 'communities', allowing for harmful behaviours to amplify and escalate**

  Unlike standard social media communities, VR communities also involve physical presence. Physical actions become part of community culture, as well as words. Charismatic influencers can rapidly foster intimacy and rapport with new members, and both healthy and harmful behaviours can be modelled through physical actions as well as words. This allows for harmful behaviour norms to rapidly emerge.[49] We believe sexual harassment and assault of children can become quickly normalised in these cultures.

  The tight-knit nature of VR communities can lead to attempts to self-police and victims are strongly discouraged from sharing their stories beyond the group. These groups can become defensive when the community is criticised by outsiders: Angus Crawford's 2022 BBC investigation reported users engaging in activity like doxxing (see glossary) as an act of retaliation against those who speak out.[50] Users can also believe that harassment is the victim's fault as they have not conformed to the community's norms.

Design characteristics that contribute to this harm

- **Most VR multi-user world safeguarding features are user driven**

  Safeguarding features often require that the victim takes immediate action after an assault or harassment incident, such as reporting it to the platform. This fails to take account of the possibility that a victim may need time to process what has happened to them, and to even classify an incident as sexual harassment or assault.

  Placing the onus on the victim to take action also ignores the possibility that victims may be discouraged from using the safety features, or from reporting harmful experiences, by their community. This theme of victims being conditioned into taking personal responsibility was observed by Sparrow (2022).[51] Sparrow's research found that in an online multiplayer (including desktop) game, players came to expect some level of abuse and harassment; regardless of the victims' or bystanders' belief that these behaviours were wrong, users had adopted an attitude of almost learned helplessness, believing that they were powerless to control the situation. In another example shared by documentary maker BrandonFM, a 17-year-old girl was doxxed by her VR 'family' in retaliation for blocking a member of the group in his twenties after he made her feel uncomfortable.[52]

- **Freedom to code and completely customise worlds in multi-user VR spaces means that the ability to virtually assault can be coded into the space by its creators**

  Some VR multi-user platforms offer high levels of customisability, which includes giving users the ability to customise their own VR space or experience by writing their own programming code. The testimony of one of VR whistle-blower Maze Marlow's interviewees described a user-designed ERP space on a popular platform where a design code forced victims to sit on a 'cube', trapping them into a position or movement action loop.[53] Customisability like this means that someone's avatar can be unwittingly trapped in a specific sexualised position.

Sexual activity between those under the legal age of consent in VR multi-user spaces

Rationale for expecting this risk

There are a number of ways that users can engage in sexual activity in VR spaces: erotic role play (ERP) is one such way. We have not observed under 16-year-olds engaging in ERP or found reported incidents of this in our literature review; however, during our primary research, we have come across numerous examples of people claiming to be under the age of 16 and soliciting ERP meet-ups in VR with other under 16-year-olds. 'Parties' are often arranged on these same groups, where children and adults appear to mix. On this basis, we believe that this is a risk that is already present.

The extent to which these risks are new

- **Unclear ages and anonymous identities**

  There is no straightforward way of knowing the age of other users in VR multi-user spaces. This means that a child who may think they are engaging in peer-to-peer ERP may in fact be interacting with an adult and be a victim of child sexual abuse; similarly, an adult may not realise they are interacting sexually with a child. Anonymity also means it is impossible for a user to know the location or identity of the people they are spending time with.

Design characteristics that contribute to this harm

- **Lack of age verification**

  Unlike real-world bars and clubs, entry to ERP spaces in VR is not age gated. Children under 16 and under 18 years of age are able to explore these VR spaces freely, without supervision, and therefore be exposed to ERP culture and the surrounding risks. Combining VR with real-world alcohol and drugs is a common occurrence in VR multi-user nightlife spaces, meaning children are also being exposed to these specific risky behaviours. This could mean that the potential for harm is akin to, if not more than, in real life.

- **Reliance on community moderation**

  The primarily community-moderated safety features on popular VR platforms mean that harms to children potentially remain unreported. It is not necessarily in children's perceived interests to report each other when they themselves are underage, or to report harmful incidents occurring within relatively small communities.

Underage access to virtual reality pornography

"The last two decades have witnessed a social experiment like no other: the first generation in which men and boys (who vastly outnumber women and girls as users) are engaging with sexual ideas, not as interpersonal experiences, but egocentrically mediated via screens which present others (women, girls, other men, boys) as anonymous third person(s)." (Professor Kathleen Richardson, Professor of Ethics and Culture of Robots and AI at De Montfort University)

"VR porn is going to change a generation. The whole development of relationships and connection and sexuality – and the organisation and order of it all – is all getting tossed up in the air.

...We're going to lose thousands and thousands of people to it. And it's only a couple of years away." (Dr Robert Weiss, sex and intimacy expert and author, speaking to The Sun)[54]

Definition

VR porn is pornographic content viewed through a VR headset, where the wearer is viewing the pornography through the eyes of one of the participants. This content is mostly pre-recorded and takes the forms of CGI animation, 360 video or interactive porn games. There are hundreds of thousands of VR porn apps and videos in existence, available for download. They range from amateur homemade 360 videos to professional, studio-produced interactive experiences. Our research found that approximately every hour a new VR porn film is uploaded onto the world's most popular online porn site.[55]

It is important to understand that consuming VR porn is substantially different to consuming porn in other formats. The majority of VR porn involves setting up a situation that enables the user to simulate being a part of the activity. VR porn is usually 'point of view', which means the user is complicit and feels involved; the impact is different to that of viewing two-dimensional porn.[56] Many VR porn users may even feel 'phantom touch'. Some VR porn users add haptic technology, ranging from commercially available devices to specialist synchronized sex toys.

What this means is that a child exposed to VR porn will simulate sex acts with an adult performer through a VR platform. Given that children cannot consent to sex with an adult, these simulations make us question whether the current law is appropriate.

Rationale for expecting this risk

While we are not aware of evidence confirming that children are exposed to VR porn, we believe this is highly likely to be the case.

A large proportion of children are already accessing 2D pornography online, with boys more likely to be viewing pornographic content.[57] Moreover, some of this online content is deliberately sought out rather than stumbled upon: a survey by BBFC found that almost three in 10 children aged 14–17 years who had seen online pornography, did so intentionally.[58] According to YouGov, in May 2022 45 per cent of UK adults reported having been first exposed to screen-based pornography below the age of 18 years old.[59] In men aged 18–29 years, the figure is 83 per cent.[60] Of note here is the fact that teenage boys and young men are also the demographic most likely to use VR.[61]

We believe that at least some children who can access VR spaces would view VR porn, either intentionally or otherwise. There are currently very few safeguards or barriers preventing this: VR porn is widely available, and 360 videos can be easily sideloaded onto VR headsets without needing to be purchased and downloaded from an app store. We suggest it is also worth considering the possibility that children may be shown this material by adults wishing to groom them; while there is currently no evidence that this is occurring, 2D pornography is already used in similar ways to normalise inappropriate interaction and sexualise children as part of a grooming process.[62] [63]

The extent to which these risks are new

- **Impact on autobiographical memory**

  We believe that viewing porn in VR – which essentially equates to simulating sex – embeds the experience in autobiographical memory. According to a 2017 psychology study into memory formation at Osnabrück University, whereas a conventional video experience remains an isolated episodic event, immersive VR experiences become part of an "extensive autobiographical associative network".[64] Emotions felt during VR experiences have higher salience than those in traditional screen media, and the experience of immersive porn on viewers is distinct to that of 2D porn.[65] We do not know how this experience may impact on a child's outlook and sexual behaviour in both the short and longer term as they grow older.

- **Simulation of sex leading to unhealthy impact on sexual development**

  As with ERP and 2D porn, it is likely that many children and young people will be exposed to VR porn before they have had any real-life experiences of sex. Similarly to 2D porn, VR porn available is often hardcore, extreme and in no way like a healthy sexual encounter in real life. There is a great deal of robust psychological research into how VR can change people's attitudes, values and behaviours[66] and, therefore, it is likely that regular exposure to VR porn will have an impact on a child's outlook and sexual behaviour in both the short and longer term as they grow older. The simulation factor (*doing*, rather than simply watching) could amplify this already problematic phenomena from 2D pornography.

Design characteristics that contribute to this harm

We have identified various design features of VR headsets that contribute to the harm and risk to children exposed to VR porn.

- **The relative ease of sideloading content that is not available on the official VR app stores**

  Sideloading unofficial content requires a medium level of technical skill, and once the process is established can be done fairly easily on several different brands of VR headset. Sideloading 360 videos is the most straightforward type of content for almost all devices, whereas sideloading apps can include more barriers as it often requires signing up for a developer account.

- **Certain VR headsets come with built-in web browsers**

  VR porn websites can be easily accessed with the built-in web browser. It is much harder for parents and educators to install web browser-specific safety software on VR headsets than standard devices, as it requires professional-level expertise to set up.

- **Lack of co-location and supervision features**

  A lack of co-location features in most VR headsets on the market positions the VR headset as a solitary device for solo user rather than as a family device. This makes parental supervision in VR feel less natural.

Child sexual abuse simulations in VR

"The unbounded nature of VR environments means that an increasingly diverse range of pornography is (and will become) available, including catering to paraphilic interests, violence and sadism. As with online environments, anonymity and fantasy role-playing are likely to facilitate disinhibited and potentially harmful behaviour...

Accessible and anonymous VR environments that allow users to experience more extreme and paraphilic material will likely normalise such behaviour...socialising the idea that sexual activity with children is acceptable."

(An excerpt from *The Future of eXtended Reality Technologies, and Implications for Online Child Sexual Exploitation and Abuse*)[67]

Definition

Virtual reality child sexual abuse (VR CSA) simulations use immersive technologies to enact child sexual abuse on virtual children. These children are sometimes 3D model depictions of real-life children, such as child actors or children known to the offender. This has obvious implications for trauma to a child and their family who could learn the child's image is being used in this way.

Another form of VR CSA simulation is so-called 'age play', where users 'perform' the role of a child to each other using child avatars to simulate sexual activity. These avatar types are sometimes described as 'loli' (girl) and 'shota' (boy) avatars, and can be bought, sold, and exchanged online. So-called 'age play' is often enacted in clubs in VR multi-user spaces and is influenced by anime and hentai culture. While real-life children are not directly harmed in these scenarios, we believed that simulated child sexual abuse may lead to contact offences against children; this extrapolates the theory – which is notably contested – that experiencing extreme material helps offenders overcome inhibitions and normalise sexual interests in children, thus removing obstacles to contact abuse.[68]

Evidence of this risk

Two decades ago, when discussing the *Prosecutorial Remedies and Other Tools to End the Exploitation of Children Act*,[69] politicians in the United States Congress predicted that the "technology will soon exist, if it does not already, to make depictions of virtual children look real"[70] for child sexual exploitation and abuse.

Twenty years later and we have now reached a stage of development where this harm is not only technically possible, but which experts and industry professionals interviewed for this research told us is happening at scale. In their interviews, law enforcement professionals suggested that the use of these simulations and the number of offenders taking part in this activity has risen significantly in the last five to 10 years. They described two ways in which offenders create and share child sexual abuse simulations: either through VR sex sandbox platforms, which offer users an array of highly customisable actions, interactivity, 3D models, and environments; or through technological modifications to characters in existing VR games, such as by modifying the character's age or actions. They cited cases where technology was used to create 3D child deepfakes (through AI face transfer technology).

It should be noted that the core, baseline technologies used by offenders for these simulations have mostly been developed by software creators for broad and general purposes, with no ill intention. However, offenders have repurposed these technologies as tools for simulating CSA.

Our research found that CSA simulator games can be bought on some widely available app purchase platforms. Some of this VR CSA simulation content is made by games studios in Japan and South Korea that specialise in the genre of 'eroge' games: the characters in these games are promoted as being over 18 years of age but are usually represented as teenage girls, often in school uniform. Privately created VR CSA simulation games, which interview participants described as more extreme and sometimes violent, were also known to be distributed on the dark web and through private networks.

"They mirror the way that contact offenders would speak about [real life] children they have access to and are abusing. There's obviously the underlying understanding that it's not a real child, but the way that they speak about these children is as if they were real." (UK specialist law enforcement investigator discussing offender groups using a sex act simulation creator)

What do we know about VR CSA simulation offender networks?

In their interviews, representatives from law enforcement reported that VR CSA simulation offenders use a range of technologies to communicate with each other. These include multi-user VR spaces, clear web online forums, private groups on mainstream social media platforms and dark web forums. Using these platforms, offenders can communicate and build groups, developing what might be described as 'community'. These communities allow offenders to share simulations of, and digital assets relating to, CSA. Dark web forums particularly involve the sharing of 3D models of virtual child victims, and entire interactive CSA scenes. One law enforcement officer told the authors of the existence of a CSA 'strip club' that was being distributed via the dark web. Sometimes these 'communities' resemble marketplaces, involving the exchange of money or cryptocurrency for VR content.

While child sex offenders have a range of backgrounds and demographics,[71] the experts we interviewed identified a set of qualities that are seemingly shared by CSA simulation offenders: they are almost always male; they tend to be highly technically literate and curious about emerging technologies; and they are often part of an online community, or several online communities, that specifically focus on CSA topics.

We were told that VR CSA simulation communities tend not to emerge from the general VR user community. Existing CSAM offenders will engage with one another on a central forum and then a subset of those users will move into VR space for their offending. Moreover, we heard that involvement in these communities can confer a sense of status. More extreme content may garner an offender with more status, and perhaps more income.

Members of online offender communities were described in interviews as "very accommodating" and "friendly"[72] towards each other. In interviews, law enforcement gave examples where if a community member goes to the group with a problem, they will "tell you how to do something or fix something that's not working".[73]

Members of the communities will often use language of ownership when sharing content they have made, such as this is "my girl" or "my boy".[74]

The extent to which these risks are new

- **The impact on offender pathways**

  VR CSA simulations pose a risk of normalising child sexual abuse, not only among offenders but in wider society. It is already well known that many forms of traditional, 2D media can influence the behaviour of its viewers and wider social norms: this is why advertising works, and as an industry is worth billions of dollars. VR content can similarly impact the attitudes,[75] values, and behaviours of those who engage with it.[76]

  VR content can have a particularly potent effect on its users, in part due to its impact on autobiographical memory.[77] In therapy, healthcare and training, industries are being built around VR's effectiveness at creating change in the participant. VR exposure therapy (VRET), for instance, can de-sensitise participants to particular triggers, reducing panic, for example, or fear. VRET has been used to treat arachnophobia, train firefighters, and reduce patients' social anxiety.

  In the case of VR CSA simulations, the impact of VR's immersion, customisation, and presence could form a pathway to real-life contact offending. Every expert consulted for this paper believed CSA simulations to be a significant risk to children offline. Professor Emma Barrett, Professor of Psychology, Security & Trust at Manchester University, explained how various well proven psychology theories show how simulated CSA increases the likelihood of a contact offence. While Professor Barrett spoke in broad terms, one applicable psychological theory that this paper's authors have subsequently identified is Embodied Cognition.[78] Embodied Cognition emphasises the role that the body plays in shaping the mind. The link between Embodied Cognition theory and virtual reality's power has been made by numerous researchers and academics over decades.[79] The theory proposes that our bodies, our physical actions, and our environments heavily influence our cognition – including perception, thinking, and language. The theory states that behaviours can *create* attitude and belief change. Simulating an action is a behaviour and, therefore, in relation to potential offender pathways, simulation of CSA could normalise and encourage real-life CSA.

- **Combination with an online community**

  A common perspective among subject experts, academics and law enforcement professionals who participated in interviews is that taking part in simulations can break down offenders' internal mental barriers towards offending. Experts who work with sexual offenders report that offenders often talk about how their tolerance changes for types of CSA: they describe how offending starts with viewing images, then video, then live camming, before moving to VR and CSA simulation. The sentiment around offender pathways is that once an offender begins VR simulation, they cannot go back. One police force's counter-CSA training lead explained that the combination of engaging in simulation together with being part of an online community that normalises inappropriate thoughts and behaviour could serve as a powerful recipe for breaking internal barriers and turning online offenders into contact offenders.

Design characteristics that contribute to this harm

- **Anonymity and ease of sideloading**

  As with previous harms in this document, anonymity and sideloading on some platforms are significant factors that make these harms possible. This is especially the case for VR platforms that can work offline and do not require a log in. Recommendations around safeguarding features and regulation will be discussed later in this paper.

AR and VR commercial avatar-based child sexual exploitation

"[The men] sit by the mirror and wait... They play music and ask if you want a free DJ, then after a while they ask to pay for you as a personal dancer for a club they want to make. They ask for your [server account] then try and hook up. The last guy who did this made me have a panic attack on stage. He asked me to be his dancer."[80] (A 15-year-old user of a popular multi-user VR space, who wished to keep her anonymity, speaking to documentary maker BrandonFM)

Definition

Child sexual exploitation (CSE) in augmented reality or virtual reality is the use of immersive technologies to sexually exploit children for commercial gain. This form of CSE involves a child inhabiting an avatar and being exposed to scenarios where they are manipulated into performing sexual content for an individual or audience. This could be through pre-recorded video, interactions in a multi-user VR world, or through live streaming (either on pornography websites or gaming platforms).

It should be noted that the anonymising quality of avatars may mean the buyers or viewers of this content do not know the true age of the victim.

Rationale for expecting this risk

Evidence that children are being sexually exploited in VR spaces is currently limited to reports of adolescent VR users engaging in VR erotic dancing for monetary gain in VR strip clubs.[81] We believe this harm may be more widespread than it appears. Bad actors have plenty of opportunity, and little by way of restriction, to recruit children to the many forms of adult sexual entertainment available in VR spaces.

Avatar-based sexual streaming is one such form of entertainment: it is fast growing and high grossing, and can have millions of subscribers, including those who are under the age of 18 years.[82] This type of entertainment involves an (adult) performer embodied by an avatar to act out stories or scenarios, usually enabled by full body tracking with sensors. The creator crafts their character for their audience over time, often building a mythological backstory. Inspired by anime, the most popular avatar-based streamers all share a similar set of characteristics: a feminine, youthful personality, the voice of a younger teenager and clothing that ranges from childlike to highly eroticised. Offenders with the money or technology skills to develop such platforms may spot the opportunity to create a business model that uses children rather than adults, exploiting child streamers to generate income from producing and livestreaming CSAM content.

Another form of sexual entertainment in VR spaces consists of virtual strip clubs and sex parties, where (adult) dancers and ERP providers can be paid for their erotic activities. VR strip clubs are run almost exactly like a real-life strip club[83] and adult entertainers can make a full-time wage from performances, especially when using body tracking.[84] Performers can also earn money by having ERP 'sex' with clients, an activity which usually takes places in lockable private rooms in the VR venue. Financial transactions occur on peer-to-peer payment apps, through gift card codes, or using freelancer booking platforms. It is easy to see the potential for offenders to recruit children to perform in these venues.

As some of these platforms have so many users who are under the age of 18 years, no age verification, and a significant number of virtual sex entertainment venues, it seems likely that there is a real risk of commercial CSE occurring in this context.

The extent to which these risks are new

- **Unknown ages and anonymity**

  The disguise that avatars offer means that CSE victims' ages can be unknown or intentionally ambiguous. This may also contribute to harm on other platforms. The leading website that allows for performers to sell subscriptions for sexual content only has age verification procedures to check the age of the account holder. When hidden behind an avatar, there is no way of knowing if the person performing is in fact the same person whose identity was verified when setting up the account. This potentially exposes a gap in safeguarding that CSE offenders can exploit. CSE buyers can also remain easily anonymous.

- **Scalability**

  VR technology offers the potential to scale-up human movement and activity, and to share performances with thousands of users at a time, globally. Moreover, there is no requirement for the same person to inhabit an avatar: once an avatar-based sexual streamer has built a brand, anonymity allows for numerous others to adopt the avatar and perform to multiple audiences. Altogether, these conditions facilitate scalability, and create the potential for a lucrative CSE business model.

Design characteristics that contribute to this harm

- **Lack of regulation and effective policing resource**

  Because the technology is in its infancy, businesses on these platforms are currently poorly regulated and policed. This can subsequently attract CSE offenders who see these spaces as safe places to offend.

- **Absence of moderation**

  As mentioned above, many VR communities often rely on peer-to-peer moderation where a user has to first notice unsafe behaviour and then act on it. However, there is a reluctance in the community to call out abusive activity, for fear of repercussions. There are also additional challenges in moderation linked to the real-time nature of interactions, ephemerality of content, and limitations in visibility, which characterise virtual reality spaces.[85]

Analysis

It is clear from the outline of these harms that without adequate safeguarding, immersive technologies pose a very real and present threat to children, especially from offenders using VR technology.

Global figures for immersive technology offender numbers are already in the hundreds of thousands, according to intelligence gathered by a long-term UK policing operation.[86] This may sound like a very large number for immersive technology; however, it tallies with broader scale of adults who pose a threat to children. In the case of the UK, the National Crime Agency's 2023 estimates, there are between 680,000 and 830,000 UK based adult offenders who pose varying degrees of risk to children, equivalent to 1.3% to 1.6% of the UK adult population.[87] We do not know how many of those offenders are likely to be using VR. What we do know is that, by the end of 2021, according to Limina Immersive's own tracker study, 4% of UK adults used VR at least once a week.[88]

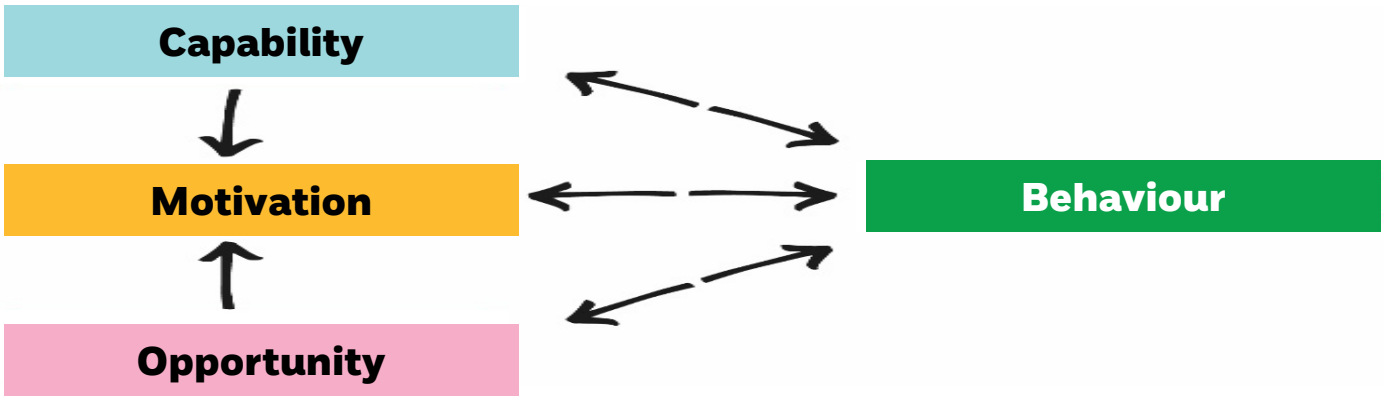
It is useful to observe this scenario with the COM-B[89] behaviour model in mind. While this model is commonly used to demonstrate how behaviour change works in general, including pro-social or beneficial behavioural change, it is a useful reference point for also understanding the circumstances leading to this sort of abuse. The COM-B behaviour model represents the observation that, at any given moment, a particular behaviour will occur only when the person concerned has the capability and opportunity to engage in the behaviour and is more motivated to enact that behaviour than any other behaviours. It is clear that the three basic conditions are in place for a growth in immersive technology facilitated offending: the capability of perpetrators, their motivation and, unfortunately, the opportunity.

UK law enforcement's Online CSA Covert Intelligence Team (OCCIT) say:

> *"Whilst this type of offending continues to grow within niche areas occupied by online sex offenders, it will likely grow...*
>
> *Virtual reality and the metaverse have the potential to be a monumental hurdle for law enforcement, criminal justice, and the safeguarding of vulnerable people. The proposed technology may have cultural implications not seen since the global explosion of internet technologies. Whilst the landscape is constantly shifting in terms of potential and expectations, we can at least somewhat foresee the issues on the horizon and prepare for them based on the misuse of the technology happening now."*[91]

This section of the paper examines this growing threat by analysing prevalent themes in the harms identified. It also outlines the current safeguarding features that technology platforms in general have already put in place to mitigate risk. This paper will finally conclude with recommendations on what policymakers can do to address this pressing issue.

- **The COM-B Behavioural Model.**



Reproduced from Michie et al (2011)[90]

Factors that contribute to the risk that children may be harmed

The harms identified in this paper have a variety of amplifying factors that compound and intensify the problem. These amplifying factors do not just affect users: they contribute to the broader culture that informs criminality and regulation (or lack of).

Cross-platform interactions

> *"The link between having a VR headset and going down the rabbit hole to a server is stupidly easy, although you will have to be a 'bit' interested in CSAM in the first place. You don't have to be technically adept."* (Convicted VR CSAM offender during interview with UK law enforcement investigator)[92]

Immersive media does not live in a vacuum and many of the actions that lead to the harm of children are happening in parallel on different platforms. An underpinning foundation to so many of the harms identified in this paper is the symbiotic relationship with phone or desktop-based social media platforms and message boards. People who use VR often use 2D social media to find out about virtual places to visit, and to talk further with people they meet. The social media platforms that VR users use are often the same platforms that many of us use every day.

In the past few years, society has witnessed the negative real-world impacts caused by social media, including polarisation, disinformation, cyber bullying, and unhealthy tight knit online communities (for instance the 'pick up artist' community[93] or the 'pro ana' community[94]). By pairing online social media platforms with VR, these unhealthy dynamics can follow through. Harmful practises in VR can then be normalised and encouraged in these 2D spaces.

Our interviews with law enforcement professionals revealed that the CSA simulations shared on 2D forums have become increasingly higher tech and realistic in nature. We think this could be due to offenders performing their success to one another: vying for status and influence in these online offender communities.

The cross-platform nature of many users' VR journeys also means that for victims of grooming, the abuse does not end when the VR headset is taken off. VR is often the start of an ongoing ordeal. Other social platforms are used to maintain contact with the victim, sometimes to arrange further meet ups in VR. It is clear that the harm must be tackled on immersive spaces and the parallel platforms.

Body disassociation and avatar transference

Disassociation is a condition associated with VR. We believe dissociation can contribute to CSA offending patterns.

VR disassociation is the experience of coming out of VR and not feeling connected anymore to one's own body, and/or perceiving the physical world as not real. This can induce anxiety, dread and even panic attacks. As far back as 2010, clinical psychology researcher Frederick Aardema investigated and identified the phenomenon in relation to VR, finding that VR increased dissociative experiences and decreased people's sense of presence in actual reality.[95] This response is most likely when the VR experience has involved body transference into an avatar.

Accounts from VR users of the disassociation they experienced, including an account from one of this paper's co-authors, show the impact of this disassociation:

> *"While standing and in the middle of a sentence, I had an incredibly strange, weird moment of comparing real life to the VR. I understood that the demo was over, but it was [as] if a lower-level part of my mind couldn't exactly be sure. It gave me a very weird existential dread of my entire situation, and the only way I could get rid of that feeling was to walk around or touch things around me."* (Video game developer Lee Vermeulen in 2014)[96]

> *"I felt like my body was not my own…I knew these were my arms and legs, but I didn't feel like I had any connection to them. As I walked downstairs I felt as if I was floating. Time had stopped moving, or I had no sense of it passing. The dissociation was so strong that I thought I might actually be going insane. Reality itself began to seem like an illusion."* (Photographer Shane McGeehan in 2018)[97]

> *"I've seen all sorts of responses to immersion, ranging from quiet discombobulation to a frenzied screaming episode. I've actually experienced depersonalisation of my own: the first time I tried Batman: Arkham VR, I came out, looked at my hands and didn't recognise them as my own."* (Author Catherine Allen writing in Wired Magazine in 2017)[98]

As well as being a phenomenon associated with VR usage, victims of physical, real-world sexual violence can experience disassociation during or after an attack.[99] This also applies to children[100] and is a well-documented response to trauma. The potential impact on victims of VR abuse could possibly involve a double disassociation. This could have wide-ranging and severe psychological effects, all of which require more research.

Disassociation can amplify harm to children because it is also likely to affect CSA offenders, and in this way contribute to their offending pattern.

> *"When you are in VR for hours and then come out, real life doesn't feel real, eating food doesn't feel real, your limbs don't feel real."* (Convicted VR CSAM offender during interview with law enforcement investigator)[101]

The impact of disassociation on offenders could include a long-term build-up effect where the constant body transference into the simulation of a person committing criminal acts creates a bodily association with that character (and a disassociation with the offenders' physical body).

Academic studies have shown that inhabiting an avatar identity of an 'outgroup' in VR can increase positive sentiment and even empathy towards that group of people.[102] The studies that demonstrated this capability in VR were using the medium for positive, pro-social outcomes. There have been beneficial outcomes of this type of VR content, including increased donations to charities.[103] However, VR's ability to generate empathy through body transference could be misapplied in the case of non-contact CSA perpetrators constantly inhabiting the VR body of a contact offender. In terms of offender pathways, feeling more positively towards contact offenders could increase the chances of someone proceeding to real-life offending.

Trivialisation

We believe that society's tendency to trivialise the metaverse and VR can allow harms in these spaces to slip under the radar.

Surveys suggest a significant proportion of the public believe that notions of the 'metaverse' and 'virtual reality' belong in the realm of science fiction and futurism.[104] These futuristic assumptions have led many to trivialise these technologies and sometimes even to refuse to engage.[105] This general trivialisation of the technologies could, in theory, have a range of impacts on parents, children, offenders and decision-makers.

For parents, the trivialisation of VR could potentially make it appear less risky, and therefore mean they are less likely to apply close supervision to their children when the child is engaging with VR. This stems from the thinking that it is 'just a game'. There is some empirical support for this theory: while exposure to inappropriate content was a concern for three quarters of parents when they were asked to reflect on children's online use,[106] fewer than half felt that this was a concern when asked to reflect on children's engagement with 'the metaverse, virtual reality or augmented reality'.[107]

Children may feel that they should 'not make a big deal' out of the harms that happen to them in VR. They may fear they will not be taken seriously, or a parent will not understand as it is 'not real'. If this is indeed the case, it could lead to a reduced likelihood of disclosing incidents to parents, carers, educators, platform moderators, or law enforcement.

At the same time, there is evidence that offenders use the fact that VR is virtual to self-justify their actions, often using variations of the phrase "it's just pixels" and referring to VR CSA as "vegan child porn" to highlight their opinion that it is apparently less harmful.[108]

Trivialisation and futuristic stereotypes are major factors in the previous lack of awareness among UK politicians of VR and the harms it poses. The trivialisation of VR and the metaverse can lead to decision makers not taking it seriously as a **present** threat, and therefore delaying meaningful research, immersive literacy education, regulation, and legislation.

Decentralised transactions and asset exchanges

Many transactions relating to virtual reality, or occurring within VR spaces, are decentralised. This creates a level of risk for children, as accountability becomes less likely without a centralised marketplace or registered seller businesses.

The sale of VR apps and content is one example of this decentralisation. The official curated VR app stores are not the only source for apps and content: while there is a mainstream userbase who do not stray from the official channels, sideloading onto most VR devices is

straightforward for those with mid-level technology skills or higher. Sideloaded content, such as VR pornography, is potentially less likely to come with any safeguards.

Commercial VR transactions are also largely decentralised. Such transactions may include the sale of venue entry, for example an entrance fee to a virtual nightclub; a user paying another user to spend time with them or for dances in a VR strip club; or paying for assets like customised avatars or character models used in dating sims or VR sex sandboxes. Commercial VR transactions happen in both traditional currency and cryptocurrency. These sales often occur through peer-to-peer decentralised transactions on separate apps and web services; even when exchanges happen in traditional currency, they tend to use intermediary peer-to-peer cash apps, or third-party sales platforms. These conditions make it difficult to pinpoint and crack down on illicit or indecent material and activity that may harm children.

Other potential factors

Two further themes should also be considered regarding AR/VR regulation and policymaking.

Both encryption and interoperability are likely to have an influence on the shape of the future metaverse and immersive technology sector. There can, of course, be a multitude of positive applications of these technological principles. However, there are also important considerations for child safety.

- **Interoperability**

  Interoperability is a characteristic of a system, platform or product that allows it to work with other systems, platforms or products. If two systems are interoperable, it means they can 'talk to one another'. In the context of immersive technologies, it means that assets, contacts, 'friends' or avatars could transfer from one metaverse platform to another. It could also mean that if an asset has economic value on one platform, its value could transfer through to another: a virtual pair of designer trainers, for instance, could be purchased in one metaverse world, virtually worn to a VR nightclub on a different metaverse platform, and then later sold in a completely different VR world.

  Interoperability inevitably will have implications to child safety on these platforms. It can mean that an offender attempting to groom a child can easily take a multiplatform approach. Much online sexual abuse is already cross-platform, with offenders beginning a grooming process on a more mainstream, moderated platform, but then transferring the grooming to a less moderated, 'darker' space.[109] Interoperability could amplify this trend even further.

  Interoperability of digital assets and attached value could potentially also lead to efficient cross-platform markets of CGI indecent images of children (IIOC), which are even harder for law enforcement agencies to tackle.

  It should be noted that the general benefits of *responsible* interoperability in AR and VR could be significant, even supporting consumer rights. However, systems must be designed in a way that does not aid perpetrators in committing digital immersive child abuse.

- **End-to-end encryption**

  Children's data privacy was emphasised by a range of expert voices as a key factor in building a safe metaverse.

  Privacy violations could cause significant detriment to a child, including through harmful targeted advertising, for example, or data sales to a bad actor. Privacy violations could also be more direct: an offender hacking into a parent's online photograph storage and using that visual material to build a realistic replica of the child via the AI tools discussed above in the CSA simulations section.

  Encryption can be a tool to support an end user's privacy, even performing a safeguarding function. It is not straightforward, however. In certain contexts, end-to-end encryption can be a barrier to safeguarding. The end-to-end encryption of platforms that children use can make it very difficult for law enforcement to gather evidence of online child abuse, giving perpetrators more of a feeling of impunity.

  End-to-end encryption is not currently particularly predominant in AR and VR spaces; however, this may change. End-to-end encryption has already been rolled out to some users.

  It is without doubt that encryption can be a powerful tool for maintaining consumers' rights to privacy; however, immersive technology policymakers must also consider how encryption can be a tool for criminals who want to harm children and evade consequence. Just like immersive technologies, encryption is powerful and must be applied thoughtfully and responsibly.

Existing safeguards for children's VR and AR experiences

There are clear, major and present issues surrounding immersive technologies that need to be urgently addressed. Addressing harm to children in VR and AR requires a multifaceted approach from different stakeholders. These stakeholders include the technology platforms, industry leaders, law enforcement, policy makers, educators, and parents.

Although as a society we are still at an early stage in the journey towards effective immersive technology regulation, there is a patchwork of mitigating measures already in place.

The good news is that most major immersive technology platforms already have some safeguarding features. Previous public information campaigns around general internet safety and children's screen time have supported many parents and caregivers in their existing approach to their children's use of VR. Laws in the UK already *do* apply to offenders in virtual spaces, such as the *Sexual Offences Act 2003*. More information about the key existing laws can be found in *Child Safeguarding and Immersive Technologies: Key Concepts*. Even if enforcing existing laws is currently a challenge, they still exist and could (and should) be utilised to protect children and prevent offending.

The protections that immersive technology platforms are already implementing include:

- **From late 2023, manufacturers for most VR headsets on the market state the minimum age will be between 10 and 13 years**

  Manufacturers state the lower age limit in their terms and conditions, and some providers are explicit that some spaces are adult-only.

- **Platforms require connection to a device**

  Some VR headset products require a mobile phone app to set the device up. One could assume this means that a nominated person is responsible for the device. Offenders steer clear of trackability and so a connection to a mobile phone deters them.

- **Acceptable behaviour is often stated from the outset by many virtual world platforms**

  Users of some platforms must take part in an induction to the space, which includes going through the policy on behavioural standards.

- **Employees or volunteers who guide users in virtual spaces**

  A VR guide's role includes elements like setting the tone, supporting users in making the most out of the platform, sharing guidance on staying safe and what acceptable behaviour is and is not. When necessary, the guide sometimes will escalate an issue. In some platforms, event organisers will often ensure there are in-person moderators or even 'bouncers', with features coded into the space to support this.

- **Block features**

  Most multi-user VR platforms allow users to completely block another person/avatar, meaning they no longer see or hear them. One issue to be aware of is that with blocking, an offensive action will likely have taken place. This makes it a reactive, not proactive, approach to safety.

- **Report functions**

  Reporting to a moderator can happen in app or through a form on the platform's website. As with blocking, this is a reactive, not proactive, safety feature.

- **Poll to remove feature**

  Most major virtual world platforms include a feature where people present in a specific space can anonymously vote to remove a disruptive individual. If the majority of the group agrees to remove the disruptive user, that person is immediately taken out of the space.

- **Safe space**

  Some platforms allow users to temporarily go into a safe personal space or straight back to the menu screen.

- **Personal boundaries**

  VR multi-user worlds often allow users to implement a personal boundary space around them, which operates as an invisible shield and does not let other people in the space close to them.

- **Sideloading content and transferring files to the device has a small amount of friction***

  While all major headset manufacturers support the playing of the users' own 360 video content, some have built in a small amount of friction for computer to headset transfers.

  Some platforms require users of sideloading apps to enter 'developer mode' and register as a 'developer'.

Immersive technology developers working for a variety of platforms have spent time considering and developing these safeguarding features, and it is likely that the presence of these features does give parents a sense of reassurance.

Limitations of the existing safeguards for children's AR and VR experiences

A whole range of measures have been put in place by immersive platforms and are likely mitigating the risks to some extent. However, on a law, policy and regulation level, existing laws and regulations built for legacy technologies are also clearly not adequate.

Some gaps and blind spots in platforms' safety measures include:

- **Platforms' safety process connections to local law enforcement are tenuous or non-existent**

  Harms to UK children are occurring in immersive environments. Despite this, victims may not be reporting all instances of harm to law enforcement, and subsequently, police do not tend to get involved. There are very few referrals linked to virtual reality platforms on the UK's National Child Protection database; in the past two years, less than 25 referrals have been made.[110]

  Social VR platforms tend to keep the reporting process 'in-house', with little transparency on the process. There is no sense of either an established independent justice system, or evidence of a meaningful attempt to integrate into the justice system in the victims' home country.

  This detachment from real world established justice systems is likely a factor in what makes immersive environments feel to many like a 'wild west' where 'anything goes.'[111]

- **Safety features place the onus on the victim**

  From blocking, to personal boundaries and vote-to-remove features, it appears that most safety features in virtual worlds are primarily victim-led. This places the onus on the victim to report harmful behaviour.

  This is a particular challenge for children. They first need to recognise that someone is perpetrating harm against them and be able to identify that the behaviour is not acceptable. Offender grooming methods are specifically designed to prevent this. An offender grooms a victim to accept and normalise harmful and abusive behaviours.

  Children also need to understand the reporting and safety features, and how to go through the reporting process. This expects a high level of awareness and initiation from the victim. Victim-led safety strategies can also lead to a victim blaming culture whereby when harms *do* happen, it is because they "didn't know how to use the safety features".

* Friction, in sideloading, is defined by Apple as "additional steps and warnings that prevent users from sideloading apps without realizing it" (p. 19). Apple Inc. (2021). *Building a Trusted Ecosystem for Millions of Apps: A threat analysis of sideloading*. Accessed on 11/08/2023 www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps_A_Threat_Analysis_of_Sideloading.pdf

- **Community self-moderation can lead to harm amplification and victim-blaming**

  Insular user communities can sometimes discourage the use of the safety features as part of their tight-knit culture, with a preference on dealing with issues internally as they arise. This attitude deters users from speaking out, with doxxing or threats of violence as 'punishment'.

  Users who disclose harmful experiences in VR on online forums often discover that these operate primarily on their own community self-moderation model. Principles that have been established on self-moderated platforms can then travel into VR worlds.

- **Access to non-app store content lacks safeguards**

  Dedicated CSA simulation content is mainly made possible through sideloading, tethered PC VR (when a VR headset is attached to or driven by the PC, rather than being stand-alone).

  It is important to note that all these options for experiencing VR outside of the official curated app stores will have many wholly legitimate use cases, for instance in education or by creative technology artists.

  However, an offender could in theory go to a high street technology store one afternoon to purchase a VR headset and by the evening they could be using that device to simulate the sexual abuse of a child.

  There is clearly a need for industry and policymaking stakeholders as a whole to consider VR's sheer power in their attitudes towards regulation. The ability to realistically simulate comes with high risks attached. Barriers to offending and deterrents should be put in place wherever possible. This could begin by addressing the 'user journey' of accessing unauthorised content. Even steps as simple as ensuring unauthorised app users know the existing law and penalties in the UK could make a difference.

Conclusion

Mitigating the risks of online harm to children in VR and AR

When this research was commissioned, the expected outcome was to identify a range of likely future risks to children through immersive technologies. The assumption was that the hazards revealed would be just on the horizon, thereby putting this research slightly ahead of the curve, leaving ample time for policymakers to assess and put in place safeguards.

Instead, it is now undeniable that certain misuses of **VR and AR pose a present threat to children**.

Some of the offender behaviours discussed by our interview participants seem more like something from a harrowing dystopian sci-fi world than activities happening in the present. The reality is that the threat is present and is likely to grow. The stakes are high, and action must be taken.

As outlined in the previous section, platforms do already include various safety and moderation features. The laws of Britain also apply: an offender taking part in illegal activity on British soil is still committing a crime, regardless as to whether they are in VR or not.

So, what is going wrong?

A key reason why this activity is able to take place is because regulation, cultural norms and law enforcement have not caught up yet. Offenders flock to places where there are fewer risks of repercussions, and to where "anything is possible".

This, combined with a lack of safety features on some platforms, has created a space where children are at risk.

But there is another reason, and it is a reason that will not necessarily go away if various authorities simply 'catch up' while maintaining an out-of-date mindset that fails to recognise the unique threats posed by immersive technology. It is that immersive technologies are fundamentally not the same as the world wide web. Some tools for ensuring safety in immersive environments might be the same as for apps and websites, but some need to be quite different. VR and AR are not just places to consume content. They are places of real-time action. Just like in real life, things happen **directly** in VR.

Most of the internet still involves the user staring at, and sometimes interacting with, a glowing rectangular screen. With AR and VR, users can *enter* it. They are not just viewing or listening or inputting information. They are doing. Rather than just using their fingers and eyes, they enter the space with their whole body. This has profound implications for victims of CSA and CSE. This vital difference needs to be reflected in our regulation and legislation.

Technical countermeasures

To protect children from present harms, and to prevent future harms, lawmakers and platforms need to build a toolkit based on actions, not a kit based only on 'content' that is being 'posted'.

The tools that will make social media and the world wide web a safer place for children will help with VR and AR, but they do not provide the full solution. Social media and web regulation take inspiration from what has worked with legacy systems like message boards, television, pamphlets, and the postal system. VR platforms often include elements of social media, so we can use tools here for part of the kit. But for the rest of it, we need to look for inspiration from elsewhere.

This, conversely, is where society can begin to enter its comfort zone. The experience that immersive technology is most like real life. Virtual worlds are currently – and will be increasingly – more like a set of venues, events, and marketplaces. There are plenty of existing laws, norms and customs to deal with offences that take place in offline spaces. Offline standards can be carried through into computer-generated spaces and how they can be enforced. Adaptation or revising may need to occur, but there are strong foundations to build upon.

From the public's perspective, it is already a common sentiment that pre-existing laws should apply in VR.[112] If this is the case, then it means VR is not necessarily the place to 'live out every wildest fantasy', as some sci-fi visions of VR suggest. Not when some of those fantasies could put other individuals at risk, cause harm, or have a destructive effect on the user.

When we look to near-future legislation, it is vital that AR and VR are clearly and meaningfully included in the enaction of the Online Safety Bill (OSB). Because the OSB is platform agnostic, we know AR and VR are included,[113] and this has been confirmed by Government ministers in both Parliament and the House of Lords. While the language in the Bill is mainly geared towards 'content' rather than real-time activity, there are still many ways it will help with making VR, AR and virtual worlds safer places.

There are numerous ways we anticipate the Bill can protect children from VR-related harms. In the case of multi-user virtual worlds, the Bill can be especially effective when providers are bound to proactively mitigate the risk of their platforms being used for illegal activity. The amendments added in July 2022 requiring a safety-by-design approach are especially important here, as action in VR happens in real time and communication is often ephemeral.

The OSB will help address underpinning issues on social media platforms. Issues borne out on these 2D platforms can subsequently manifest themselves in VR. The Bill will help address these issues at the root. For the first time, user-to-user platforms, which include many worlds in the metaverse, will have a legal obligation and financial incentive to disrupt and tackle CSA on their platform.

Further, the Bill has scope to significantly reduce children's access to VR pornography through its age assurance duties, child safety duties, and duties relating to pornographic content.

Deepfake pornography is also included in the Bill. The amendments recommended by the Law Commission in November 2022[114] will help tackle deepfake CSA simulations in VR. People who share deepfakes could be jailed under this new legislation.

On top of this, the Bill has the potential to aid in getting CSA simulation files and assets that are hosted online and downloaded via the web taken down. This is less certain, however, as the files are often shared in closed insular offender communities on small scale forum services, sometimes on the dark web.

The Bill also brings the possibility of increasing transparency in the moderation and reporting process and ensuring that user reports of harm are acted upon.

Despite the opportunities offered by the Bill, it will still be at least 18 months from the time of this report's publication until the relevant parts of the Bill are implemented (after royal assent). Eighteen months is a long time in the context of emerging technology growth and adoption. There is a crucial window of time where children are highly vulnerable. In this window of time, law enforcement must be given extra resources to implement the existing laws that already apply to these spaces.

Even after the OSB comes into force, the legal toolkit will still need bolstering. Other laws may require amendments, policing techniques may need to be trialled, further regulatory approaches might need to be developed, new sentencing guidance written, and we may also need fresh legislation specific to immersive technology.

VR can be potent. Certain experiences can even generate effects akin to drugs. If a developer, for instance, wants to create an experience that achieves a particular mood or behavioural change in a user, then they have much of the ability to do so. This technology is powerful, and to truly protect children, immersive technologies must be regulated and safeguarded in a range of ways. There is so much positive potential that immersive technologies can offer children, families, and society as a whole. However, unless our human rights carry through into immersive space, this vast potential will not be realised.

Recommendations

The paper authors, and the NSPCC, hope this paper will both sound the alarm and stimulate early ideas for how to address these pressing questions. The aim is to open the conversation and begin the process of action being taken.

Based on the paper findings, the NSPCC has prepared a set of recommendations, with support from Limina Immersive, for government, the regulators, law enforcement, and the technology sector to consider.

Recommendations for UK government

1 Review legislation on a rolling basis to ensure that emerging harms are adequately covered.

Immersive environments will continue to develop rapidly, and it is possible that new design features could be outside the scope of the Online Safety Act. It is essential that the legislation is reviewed on an ongoing basis to ensure that it works in practice and is up to date.

Reviews must consider how immersive environments are covered by legislation and the role that app stores play in facilitating harm to children.

2 Consider whether there is a case for creating new offences for simulated abuse.

The Ministry of Justice should review existing offences to understand how simulated offences are covered, and if further legislation is required. These offences could include simulated rape and assault.

As discussed in our supplementary paper, *Child Safeguarding & Immersive Technologies: Key Concepts*, Europol Innovation Lab raises concerns on whether current legislation can appropriately respond to the harms on the metaverse.[115] The report also notes that:

> *"It will be important to have a clear idea of what is to be considered criminal behaviour in the metaverse and to have matching laws to provide the means to prosecute these transgressions." (p17)*

3 Ensure that child safety is factored into all policy making related to emerging technologies.

The last 20 years of the development of online spaces have shown us that children's safety is often considered as an afterthought. It is important that child protection is seen as a key pillar of policy making and on par with innovation. We encourage policy makers to engage with children, survivors and the organisations that represent these groups.

4 Build an understanding of immersive technologies among decision makers and safeguarding professionals.

Promote immersive literacy across departments through the use of VR headsets and AR devices. Regularly gain hands-on experience with emerging consumer-facing technologies.

5 Provide more guidance, funding and learning opportunities to local law enforcement for how to appropriately respond to simulated offences, including those in VR.

Upskilling law enforcement is critical in the response to the new and emerging risks. The Home Office should invest in upskilling police forces for dealing with this sort of emerging technology threat. As noted by Europol,[116] exposure to the technology will be a vital tool in supporting law enforcement to appropriately assess and respond to threats.

Recommendations for UK regulators

1 Ofcom should engage with immersive technologies as a distinct form of media.

a) VR and AR should not be conflated with other forms of new media (e.g. social media). Regulators, such as Ofcom, **must focus on balancing privacy and security concerns for age assurance and safety in immersive environments.**

b) To effectively regulate VR and AR technologies and address the challenges they present, it is **crucial for regulators to understand how threat is different in immersive environments.** Regulators should look to increase their understanding of the technical aspects and potential future developments of these technologies. This can be achieved by upskilling regulators with experts who specialise in immersive technologies.

c) Ofcom should **produce a regulator 'state of the nation' report on emerging technology risks**. This would shine a spotlight on the new and emerging risks and help communicate the risks to society.

2 Ofcom should respond to the risks of immersive environments in regulation.

a) Ofcom should work closely with other UK regulatory bodies to **develop clear guidance on how immersive technology platforms should assess and respond to risks** on their products.

b) Ofcom should l**ook to issue a dedicated code of practice on immersive environments and third-party VR apps**. This code should also look to consider challenges surrounding interoperability, artificial intelligence, and cryptocurrencies.

c) Ofcom should look to **issue specific guidance on tackling cross-platform risks**. Contact abuse often takes place on multiple platforms, and we expect the same to be true in the metaverse. The regulator should provide guidance for how platforms should address cross-platform risk appropriately. It should also consider what cross-platform risk means for interoperable immersive spaces.

d) Ofcom should use its new regulatory powers to **provide clear age assurance guidance** on how to safely enforce minimum age thresholds in immersive environments.

3 Ofcom to consider the role that VR app stores can play in keeping children safe.

Under the Online Safety Bill, Ofcom will be required to produce a report about the use of app stores by children. This report must also cover the way that app stores are used, and can facilitate harm, in immersive environments.

Recommendations for UK law enforcement

1 Increased dialogue between civil society and law enforcement.

Greater dialogue between civil society bodies, with a focus on safeguarding users online, and law enforcement officials could ensure companies have the safety of children, and other users, as a priority at each stage of product development. Dialogue between these two bodies is considered "essential" by the Europol Innovation Lab in encouraging a safer build of the metaverse (p26).[117]

2 Increased engagement on the metaverse.

We support the Europol Innovation Lab's view that law enforcement should increase engagement on the metaverse and gather "invaluable insights" on the technology (p26).[118] According to Europol, increased familiarity with the technology will allow law enforcement officials to "stay informed on the subject and enable them to assess developments accurately, answering threats as they emerge" (p26).[119]

Recommendations for the technology sector

1 Implement safety-by-design across all VR and AR products.

The tech sector plays a pivotal role in mitigating risks and creating a culture of safety by design in the metaverse. This includes building robust safety features and reporting systems. Companies should regularly monitor the efficacy of these features, being transparent about their use, and considering cross-platform risks for their users.

Safety-by-design features could include:

- Age assurance and verification
- Age-appropriate content and spaces
- Human moderation so that the onus is not on victims or witnesses to report after an offence has taken place

2 Foster a proactive approach to child safeguarding in immersive environments.

a) Safeguarding features should not be solely user-driven, especially for users aged under 18 years and should involve parents when appropriate. We encourage platforms to meaningfully engage with children, survivors and the organisations that represent them to form better design choices.

b) Data collection and sharing practices must protect children's data and adhere to the ICO's age-appropriate design code.

c) Companies should provide assurance and training for community moderators to reduce risks posed by bad actors. Age assurance measures should be built-in to products, with safeguarding being the company's responsibility, not solely that of the user.

d) Reporting methods should be proactive and child-friendly, utilising user-friendly methods, such as tutorials or interactive demonstrations.

3 Transparency in the reporting and moderation process.

a) Platforms should promote a positive culture of reporting. Easily accessible routes for users to make complaints, flag harmful behaviour, and seek immediate recourse should be a fundamental requirement on all platforms.

b) Platforms should also look to build strong communications with law enforcement where appropriate. This includes reporting safeguarding concerns on their platforms to organisations, such as the UK's National Crime Agency, National Centre for Missing & Exploited Children, and other appropriate law enforcement bodies.

4 Include easy to use parental supervision co-location features and improve parental education.

Dual device co-location features would allow parents and their children to enter VR spaces together, turning the experience into an opportunity for quality family time. Funding from major VR platforms for programmes that educate parents and caregivers about the risks and how to mitigate them would make a significant positive impact. This could occur through schools and/or charities.

5 More data needs to be made available to civil society.

Increased access to data is essential in allowing civil society and academics to appropriately capture emerging harms and their scale. At the least, companies should provide greater data transparency on the platform's child user base, the child sexual exploitation and abuse (CSEA) activity detected on the platform, and CSEA reporting on the platform.

References

1 NSPCC (2021) *Preventing child abuse together: Our strategy from 2021 onwards.* London: NSPCC. Available from: www.nspcc.org.uk/globalassets/documents/strategy/strategy-2021-31-summary-booklet.pdf [accessed 21/06/23].

2 The Institution of Engineering and Technology (2022) *Safeguarding the metaverse*. London: IET. Available from: www.theiet.org/media/9836/safeguarding-the-metaverse.pdf [accessed 21/06/23].

3 Limina Immersive (2018) *Immersive Content Formats for Future Audiences.* Bristol: Limina Immersive. Available from: www.immerseuk.org/wp-content/uploads/2018/07/Immersive_Content_Formats_for_Future_Audiences.pdf [accessed 21/06/23].

4 West, R. & Michie, S. (2020) *A brief introduction to the COM-B Model of behaviour and the PRIME Theory of motivation*. Qeios.

5 Manay, N. & Collin-Vézina, D. (2021) Recipients of children's and adolescents' disclosures of childhood sexual abuse: A systematic review. *Child Abuse & Neglect*, Vol. 116, Part 1, 104192.

6 Adams-Clark, A.A., Rosenthal, M.N. & Freyd, J.J. (2020) Out-of-body experience: Sex-based harassment linked to general dissociation, sexual dissociation, and sexual communication. *Equality, Diversity and Inclusion*, Vol. 39 (1), pp38-52.

7 Limina Immersive (2021) *Limina's 2021 tracker*. Bristol: Limina Immersive.

8 Rees, K. (2022) *These 8 tech giants have invested big in the metaverse* [online]. Available from: www.makeuseof.com/companies-investing-in-metaverse/ [accessed 21/06/23].

9 Rideout, V., Peebles, A., Mann, S., & Robb, M.B. (2022) *Common Sense census: Media use by tweens and teens, 2021*. San Francisco, CA: Common Sense. Available from: www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf [accessed 11/08/23].

10 Meta blog authors (2023) *Introducing new parent-managed Meta accounts for families* [online]. Available from: www.meta.com/en-gb/blog/quest/meta-accounts-parent-managed-families/ [accessed 24/06/23].

11 Cameron, I. (2022) *Teens are split on the metaverse and the majority barely use VR headsets* [online]. Charged. Available from: www.chargedretail.co.uk/2022/04/14/teens-are-split-on-the-metaverse/ [accessed 16/08/23].

12 Ofcom (2023) *Technology Tracker 2023 data tables*. Available from: www.ofcom.org.uk/__data/assets/pdf_file/0016/262510/technology-tracker-2023-data-tables.pdf [accessed 06/07/23].

13 Rideout, V., Peebles, A., Mann, S., & Robb, M.B. (2022) *Common Sense census: Media use by tweens and teens, 2021*. San Francisco, CA: Common Sense. Available from: www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf [accessed 11/08/23].

14 Limina Immersive and IET (2022) *Safeguarding the Metaverse.*

15 Sum of Us (2022) *Metaverse: Another cesspool of toxic content.* Available from: www.eko.org/images/Metaverse_report_May_2022.pdf [accessed 21/06/23].

16 Center for Countering Digital Hate (2023) *Horizon Worlds exposed. Bullying, sexual harassment of minors and harmful content are rife in Meta's flagship VR product.*

17 Center for Countering Digital Hate (2021) *New research shows Metaverse is not safe for kids*. Available from: https://counterhate.com/blog/new-research-shows-metaverse-is-not-safe-for-kids/ [accessed 21/06/23]

18 For example, Center for Countering Digital Hate (2023) *Horizon Worlds exposed. Bullying, sexual harassment of minors and harmful content are rife in Meta's flagship VR product*.

19 Center for Countering Digital Hate (2021) *New research shows Metaverse is not safe for kids.* Available from: https://counterhate.com/blog/new-research-shows-metaverse-is-not-safe-for-kids/ [accessed 21/06/23]

20 Regli, B., Mitkus, M. & D'Ovidio, R. (2012) *Real Crimes in Virtual Worlds*, US Bureau of Justice Assistance.

21 An analysis of police-recorded offences of Sexual Communication with a Child obtained through FOIA requests in 2021/22 found that Snapchat, Facebook, Instagram, and WhatsApp were widely involved in offences.

22 Europol (2020) *Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic.*

23 NSPCC (2022) *Online grooming crimes have risen by more than 80% in four years.* Available from: www.nspcc.org.uk/about-us/news-opinion/2022/online-grooming-crimes-rise/ [accessed 21/06/23].

24 Wager, N., Armitage, R., Christmann, K., Gallagher, B., Ioannou, M., Parkinson, S., Reevers, C., Rogerson, M. & Synnott, J. (2018) *Rapid evidence assessment: quantifying the extent of online-facilitated child sexual abuse: Report for the Independent Inquiry into Child Sexual Abuse.* University of Huddersfield.

25 Office for National Statistics (2020) Child sexual abuse – Appendix tables, Table 36. Available from: www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/childsexualabuseappendixtables [accessed 21/06/23].

26 NSPCC (2023) *We're calling for effective action in the Online Safety Bill as child abuse image crimes reach record levels.* [online] Available from: www.nspcc.org.uk/about-us/news-opinion/2023/2023-02-22-were-calling-for-effective-action-in-the-online-safety-bill-as-child-abuse-image-crimes-reach-record-levels/ [accessed 21/06/23].

27 Barrett, E. (2023) *Extended Reality technologies and child sexual exploitation and abuse. Intelligence briefing for the WeProtect Global Alliance.* Available from: https://www.weprotect.org/library/extended-reality-technologies-and-child-sexual-exploitation-and-abuse/ [accessed 21/06/23].

28 Sharp, R. (2020) Louisiana man, 36, is arrested when Florida parents discover he has been living in their 15-year-old daughter's closet for more than a MONTH after he met the teen online two years ago and travelled to meet her for sex. [online] Daily Mail. Available from: www.dailymail.co.uk/news/article-8789849/Louisiana-man-living-15-year-old-Florida-girls-closet-MONTH.html [accessed 21/06/23].

29 Crawford, A. (2022) *Metaverse app allows kids into virtual strip clubs.* [online] BBC News. Available from: www.bbc.co.uk/news/technology-60415317 [accessed 21/06/23].

30 Dickson, E.J. (2021) *Inside the Underground Strip-Club Scene on Kid-Friendly Gaming Site Roblox.* [online] Rolling Stone. Available from: www.rollingstone.com/culture/culture-features/roblox-virtual-strip-clubs-condo-games-sex-1197237/ [accessed 21/06/23].

31 BrandonFM (2022) *Exposing a VR Cult.* [online] BrandonFM YouTube channel. Available from: www.youtube.com/watch?v=lGv_mXW5HIo [accessed 21/06/23].

32 DeMarco, J., Sharrock, S., Crowther, T. & Barnard, M. (2018) *Behaviour and characteristics of perpetrators of online-facilitated child sexual abuse and exploitation. A rapid evidence assessment.* Independent Inquiry Child Sexual Abuse.

33 Pettifer, S., Barrett, E., Marsh, J., Hill, K., Turner, P. & Flynn, S. (2022) *The Future of eXtended Reality Technologies, and Implications for Online Child Sexual Exploitation and Abuse.* Manchester: University of Manchester

34 YouGov (2022) *Unlocking the Metaverse.* Limina Immersive (2021) *2021 tracker survey.* Bristol: Limina Immersive.

35 Researcher interview with Michael Sheath (2022), independent consultant.

36 For access to references, see "Note on reading."

37 YouGov Profiles (2022) *Unlocking the Metaverse, An analysis into UK & US attitudes about the buzzy new technology*. YouGov.

38 Bokinni, Y. & Rice, K. (2022) *Inside the Metaverse, are you safe?* Channel 4 Dispatches.

39 Bokinni, Y. & Rice, K. (2022) *Inside the Metaverse, are you safe?* Channel 4 Dispatches.

40 Sparrow, L., Antonellos, M., Gibbs, M. & Arnold, M (2020) *From 'Silly' to 'Scumbag': Reddit Discussion of a Case of Groping in a Virtual Reality Game*, Proceedings of the 2020 DiGRA International Conference: Play Everywhere, The Digital Games Research Association.

41 Sharkey, N., Goodman, M. & Ross, N. (2010) The Coming Robot Crime Wave. *Computer*, 43(8), pp116–115.

42 BrandonFM (2022) *Exposing a VR Cult.* BrandonFM YouTube channel. [online] Available from: www.youtube.com/watch?v=lGv_mXW5HIo [accessed 21/06/23].

43 Crawford, A. (2022) *Metaverse app allows kids into virtual strip clubs.* [online] BBC News. Available from: www.bbc.co.uk/news/technology-60415317 [accessed 21/06/23].

44 Center for Countering Digital Hate (2021) *New research shows metaverse not safe for kids.* Available from: https://counterhate.com/blog/new-research-shows-metaverse-is-not-safe-for-kids/ [accessed 21/06/23].

45 Outlaw, J. & Duckles, B. (2017) *Why Women Don't Like Social Virtual Reality. A study of safety, usability and self-expression in Social VR.* The Extended Mind.
46 For access to this reference, please see "Note on reading."
47 Suler, J. (2004) The online disinhibition effect. *Cyberpsychology and Behavior*, 7(3), pp321–326.
48 Lapidot-Lefler, N. (2012) Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition. *Computers in Human Behaviour*, 28(2) pp434–443.
49 BrandonFM (2022) *Exposing a VR Cult*. BrandonFM YouTube channel. [online] Available from: www.youtube.com/watch?v=lGv_mXW5HIo [accessed 21/06/23].
50 Crawford, A. (2022) *Metaverse app allows kids into virtual strip clubs.* [online] BBC News. Available from: www.bbc.co.uk/news/technology-60415317 [accessed 21/06/23].
51 Sparrow, L., Antonellos, M., Gibbs, M. & Arnold, M (2020) *From 'Silly' to 'Scumbag': Reddit Discussion of a Case of Groping in a Virtual Reality Game*, Proceedings of the 2020 DiGRA International Conference: Play Everywhere, The Digital Games Research Association.
52 BrandonFM (2022) *Exposing a VR Cult*. BrandonFM YouTube channel. [online] Available from: www.youtube.com/watch?v=lGv_mXW5HIo [accessed 21/06/23].
53 For access to references, see "Note on reading."
54 Harrison, G. (2018) *A generation of people won't leave their bedrooms once virtual reality porn becomes mainstream, warns expert.* The Sun. [online].
55 For access to references, see "Note on reading."
56 Simon, S. & Greitemeyer, T. (2019) The impact of immersion on the perception of pornography: A virtual reality study. *Computers in Human Behavior*, 93, pp141–148.
57 Thurman, N. & Obster, F. (2021) The regulation of internet pornography: What a survey of under-18s tells us about the necessity for and potential efficacy of emerging legislative approaches. *Policy & Internet*, 13(3), pp415–432.
58 British Board of Film Classification (2020) *Young people, Pornography & Age-verification.* Available from: www.revealingreality.co.uk/wp-content/uploads/2020/01/BBFC-Young-people-and-pornography-Final-report-2401.pdf [accessed 10/07/23].
59 YouGov (2022) *YouGov Survey Results for Pornography*. YouGov website.
60 YouGov (2022) *YouGov Survey Results for Pornography.* YouGov website.
61 Limina Immersive (2022) *Ipsos study.* Bristol: Limina Immersive.
62 Researcher interview with Michael Sheath (2022), independent consultant.
63 Kloess, J., Hamilton-Giachritsis, C. & Beech, A. (2019) Offense processes of online sexual grooming and abuse of children via internet communication platforms. *Sexual Abuse: A Journal of Research and Treatment*, 31(1), pp73–96.
64 Schöne, B., Wessels, M. & Gruber, T. (2017) Experiences in Virtual Reality: a Window to Autobiographical Memory. *Current Psychology*, 38, pp715–719.
65 Simon, S. & Greitemeyer, T. (2019) The impact of immersion on the perception of pornography: A virtual reality study. *Computers in Human Behavior*, 93, pp141–148.
66 Bailenson, J. (2020) *The Experience Machine*. The Garage.
67 Pettifer, S., Barrett, E., Marsh, J., Hill, K., Turner, P. & Flynn, S. (2022) *The Future of eXtended Reality Technologies, and Implications for Online Child Sexual Exploitation and Abuse*. Manchester: University of Manchester
68 Pettifer, S., Barrett, E., Marsh, J., Hill, K., Turner, P. & Flynn, S. (2022) *The Future of eXtended Reality Technologies, and Implications for Online Child Sexual Exploitation and Abuse*. Manchester: University of Manchester
69 US Government (2003) Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today, Act of 2003. US Government
70 Al-Alosi. H. (2017) *Virtual child pornography could help and hinder law enforcement. The Conversation. [*online] Available from: https://theconversation.com/virtual-child-pornography-could-both-help-and-hinder-law-enforcement-82746 [accessed 21/06/23].
71 DeMarco, J., Sharrock, S., Crowther, T. & Barnard, M. (2018) *Behaviour and characteristics of perpetrators of online-facilitated child sexual abuse and exploitation. A rapid evidence assessment.* Independent Inquiry Child Sexual Abuse.
72 Researcher interview with specialist law enforcement officer.
73 Researcher interview with specialist law enforcement officer.
74 Researcher interview with specialist law enforcement officer.

75 Nikolaou, A., Schwabe, A. & Boomgaarden, H. (2022) Changing social attitudes with virtual reality: a systematic review and meta-analysis. *Annals of the International Communication Association*, 46(1), pp30–61.
76 BrandonFM (2022) *Exposing a VR Cult*. BrandonFM YouTube channel. [online] Available from: www.youtube.com/watch?v=lGv_mXW5HIo [accessed 21/06/23].
77 Schöne, B., Wessels, M. & Gruber, T. (2019) Experiences in Virtual Reality: a Window to Autobiographical Memory. *Currant Psychology*, *38*, pp715–719.
78 Varela, F., Thompson, E. & Rosch, E. (1993) *The Embodied Mind: Cognitive Science and Human Experience*. MIT Press.
79 Riva, G. (2008) From virtual to real body: virtual reality as embodied technology. *J. Cyber Ther. Rehabil*, 1, pp7–22.
80 BrandonFM (2021) *The Secrets of VR Chat*. BrandonFM YouTube channel. [online].
81 Dickson, E.J. (2021) *Inside the Underground Strip-Club Scene on Kid-Friendly Gaming Site Roblox*. [online] Rolling Stone. Available from: www.rollingstone.com/culture/culture-features/roblox-virtual-strip-clubs-condo-games-sex-1197237/ [accessed 21/06/23].
82 Virtual YouTuber Wiki.
83 Sung, M. (2021) *What's it like to dance in a VR strip club.* Mashable. [online]. Available from: https://mashable.com/article/virtual-reality-strip-clubs-vrchat [accessed 21/06/23].
84 For access to references, see "Note on reading."
85 Sabri, N., Chen, B., Teoh, A., Dow, S.P., Vaccaro, K. & ElSherief, M. (2023) *Challenges of moderating social virtual reality*. In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23), April 23–28, 2023, Hamburg, Germany.
86 Researcher interview with specialist law enforcement officer.
87 National Crime Agency (2023), *National Strategic Assessment 2023 for Serious and Organised Crime*. Accessed 18/08/2023 on www.nationalcrimeagency.gov.uk/nsa NCA
88 Limina Immersive (2021) *2021 tracker.* Bristol: Limina Immersive.
89 West, R. & Michie, S. (2020) *A brief introduction to the COM-B Model of behaviour and the PRIME Theory of motivation*. Qeios.
91 OCCIT (2022) *Current Misuse of Virtual Reality Technologies by Child Sex Offenders.* OCCIT.
92 OCCIT (2022) *Current Misuse of Virtual Reality Technologies by Child Sex Offenders.* OCCIT.
93 Dayter, D. & Rüdiger, S. (2016) Reporting from the Field: The Narrative Reconstruction of Experience in Pick-up Artist Online Communities. *Open Linguistics*, 2016; 2, pp337–351.
94 Brotsky, S.R. & Giles, D. (2007) Inside the "pro-ana" community: a covert online participant observation. *Eating disorders*, 15(2), pp93–109.
95 Aardema, F., O'Connor, K., Côté, S.& Taillon, A. (2010) Virtual reality induces dissociation and lowers sense of presence in objective reality, *Cyberpsychological Behaviour Soc Network*, 13(4), pp429–435.
96 Vermeulen, L. (2014) *VR and Steam Days*. 3D Element. [online]. Available from: www.3delement.com/?p=332 [accessed 21/06/23].
97 McGeehan, S. (2018) *Virtual Reality and Disassociation*. The Dreaming State. [online]. Available from: www.thedreamingstate.com/2018/02/15/virtual-reality-dissociation/ [accessed 21/06/23].
98 Allen, C. (2017) It's time to prepare yourself for VR panic. Wired. [online]. Available from: www.wired.co.uk/article/catherine-allen-virtual-reality [accessed 21/06/23].
99 Adams-Clark, A.A., Rosenthal, M.N. & Freyd, J.J. (2020) Out-of-body experience: Sex-based harassment linked to general dissociation, sexual dissociation, and sexual communication. *Equality, Diversity and Inclusion*, Vol. 39 (1), pp38–52.
100 Kisiel, C.S. & Lyons, J.S. (2001) Dissociation as a Mediator of Psychopathology Among Sexually Abused Children and Adolescents. *American Journal of Psychiatry*, 158, pp1,034–1,039.
101 OCCIT (2022) *Current Misuse of Virtual Reality Technologies by Child Sex Offenders*. OCCIT
102 Maister, L., Slater, M., Sanchez-Vives, M.V. & Tsakiris, M. (2014) Changing bodies changes minds: owning another body affects social cognition. *Trends in Cognitive Sciences*, 19(1), pp6–12.
103 Kristofferson, K., Daniels, M.E. & Morales, A.C. (2022) Using virtual reality to increase charity donations. *Marketing Letters*, 33(1), pp75–87.
104 YouGov (2022) *Unlocking the Metaverse*. YouGov.
105 Limina Immersive (2022) *Ipsos study*. Bristol: Limina Immersive.
106 Ofcom (2023) *Children and Parents: Media use and attitudes report 2023*.

107 Vibert, S. & Bissoondath, A. (2023) A whole new world? Towards a child-friendly Metaverse. Internet Matters. Available from: www.internetmatters.org/wp-content/uploads/2023/01/Internet-Matters-Metaverse-Report-Jan-2023.pdf [accessed 21/06/23].

108 OCCIT (2022) *Current Misuse of Virtual Reality Technologies by Child Sex Offenders*. OCCIT.

109 This is a technique used by adults who groom children online and is sometimes referred to as 'off-platforming'. We Protect Global Alliance (2021) *Global threat assessment. Working together to end the sexual abuse of children online.*

110 OCCIT (2022) *Current Misuse of Virtual Reality Technologies by Child Sex Offenders*. OCCIT.

111 Hughes, A. (2022) *Addiction, crime and data breaches: The metaverse could become a wild west if we're not careful. An interview with David Reid, a professor of AI and spatial computing at Liverpool Hope University.* [online]. Available from: www.sciencefocus.com/future-technology/addiction-crime-and-data-breaches-the-metaverse-could-become-a-wild-west-if-were-not-careful/ [accessed 10/07/23].

112 Schwinninger Ladak, R. (2022) *Presentation to the EU Commission at Data Centre; Savanta (2017) Wiggin Virtual Reality Ethics survey.* Available from: https://savanta.com/knowledge-centre/poll/wiggin-virtual-reality-ethics-survey/ [accessed 21/06/23].

113 Woods, L. & Perrin, W. (2022) *Regulating the future: the Online Safety Bill and the Metaverse*. Carnegie Trust.

114 Law Commission (2021) *Reform of the communications offences.* Law Commission website. [online].

115 Europol (2022) *Policing in the metaverse: what law enforcement needs to know, an observatory report from the Europol Innovation Lab*. Available from: www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know [accessed 13/07/23].

116 Europol (2022) *Policing in the metaverse: what law enforcement needs to know, an observatory report from the Europol Innovation Lab*. Available from: www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know [accessed 13/07/23].

117 Europol (2022) *Policing in the metaverse: what law enforcement needs to know, an observatory report from the Europol Innovation Lab*. Available from: www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know [accessed 13/07/23].

118 Europol (2022) *Policing in the metaverse: what law enforcement needs to know, an observatory report from the Europol Innovation Lab*. Available from: www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know [accessed 13/07/23].

119 Europol (2022) *Policing in the metaverse: what law enforcement needs to know, an observatory report from the Europol Innovation Lab*. Available from: www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know [accessed 13/07/23].

NSPCC

Together, we can stop child abuse and neglect – by working with people and communities to prevent it, transforming the online world to make it safer for children, and making sure every child has a place to turn for support when they need it.

We campaign for change. We work with schools to help children understand what abuse is and support them to speak out. Childline is here, whenever young people need us. And the NSPCC Helpline is ready to respond to adults with any worry about a child. We develop services in local communities to stop abuse before it starts and help children recover, so it doesn't shape their future.

And, above all, we work together – because everyone has a part to play in keeping children safe. Every pound you raise, every petition you sign, every minute of your time, will make a difference.

Together, we can change children's lives.

nspcc.org.uk

EVERY CHILDHOOD IS WORTH FIGHTING FOR