American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Interdisciplinary Frameworks for Protecting Children in Immersive Digital Worlds

Dr. Elena Moreau

Associate Professor, University of Lyon, Lyon, France

Abstract

Immersive digital worlds are expanding the ways children learn, play, socialize, create, and communicate. Social virtual reality, extended-reality games, mixed-reality environments, avatar-based communities, spatial computing systems, and emerging metaverse-like platforms can provide meaningful opportunities for creativity, education, social connection, and collaborative participation. Their embodied and persistent characteristics, however, also create child-protection challenges that cannot be addressed adequately through conventional content moderation alone. Risks may involve harassment, grooming, age-inappropriate interaction, manipulative engagement, biometric and behavioral data collection, privacy loss, unsafe physical movement, harmful commercial practices, developmental mismatch, and difficulties obtaining timely assistance during immersive incidents. Current policy developments increasingly support safety-by-design, privacy-protective defaults, age-appropriate experiences, accessible reporting, risk assessment, and stronger governance for services used by minors.

This study develops an interdisciplinary Child-Centered Immersive Protection Framework (CCIPF) integrating developmental psychology, human–computer interaction, cybersecurity, privacy engineering, content governance, age assurance, parental mediation, digital literacy, and children's rights. Because no original participant dataset was available, the study employs an explicitly simulation-based comparative methodology. Four hypothetical protection architectures are assessed across six dimensions: developmental appropriateness, safety-by-design, privacy and data minimization, age assurance, moderation and reporting, and child–parent empowerment.

The simulated Composite Protection Score rises from 39 for fragmented reactive protection to 89 for the integrated child-centered framework. A weighted protective-capacity model further illustrates the complementary contribution of six safeguard domains. The study concludes that immersive child safety should be designed as a layered ecosystem rather than a collection of isolated controls. Effective protection requires upstream risk reduction, age-sensitive defaults, privacy-preserving safeguards, real-time intervention capabilities, accountable governance, meaningful parental support, and direct participation by children in the design and evaluation of immersive environments.

Keywords: immersive digital worlds, child online safety, virtual reality, extended reality, metaverse, safety-by-design, children's privacy, age assurance, digital safeguarding

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

1. Introduction

Immersive technologies are progressively changing the relationship between children and digital environments. Unlike conventional websites or two-dimensional social platforms, virtual reality and extended-reality systems can place users inside interactive three-dimensional spaces where avatars move, speak, gesture, collaborate, compete, purchase virtual items, create objects, and interact with strangers in real time. UNICEF's analysis of the metaverse and extended reality recognizes both meaningful opportunities and emerging risks for children and argues that the best interests of the child should be incorporated into the development of these technologies. Research on teenagers and children in social VR likewise demonstrates that immersive environments can support social connection, exploration, play, and relationships while simultaneously creating distinctive safety challenges.

The same qualities that make immersive environments compelling can intensify harmful experiences. Embodied presence can make verbal or spatial harassment feel more immediate than equivalent interaction on a text-based platform, while real-time voice, avatar proximity, gesture, spatial movement, and haptic or sensory features introduce new pathways through which users may intimidate, manipulate, or intrude upon others. Research by Maloney, Freeman, and Robb identified concerns involving harassment, privacy, inappropriate environments, and interaction between children and adults in social VR. More recent social-VR safety research has documented multiple categories of safety risk and shown that platform safety features need to respond to the distinctive multimodal nature of immersive interaction. Australia's eSafety Commissioner similarly emphasizes that immersive three-dimensional environments can amplify existing forms of harm and that protection should be designed proactively rather than added only after incidents occur.

Privacy introduces an additional layer of complexity. Immersive technologies may process information generated through headsets, controllers, cameras, microphones, body movement, gaze, hand tracking, facial expression, voice, device identifiers, spatial mapping, and social interaction. An empirical analysis of 500 VR applications by Guo and colleagues identified security and privacy weaknesses and inconsistencies between actual data practices and privacy-policy representations. Cao and colleagues' interviews with parents of children who used VR further showed that parents often relied heavily on verbal education while encountering practical limitations in existing parental-control mechanisms; their study argued for cooperation among parents, educators, technology companies, and governments. Such evidence demonstrates why children's privacy in immersive systems cannot be protected solely through lengthy notices or parental consent screens.

Regulatory approaches are also moving toward more systemic protections. The European Commission's 2025 guidelines under the Digital Services Act recommend measures including private-by-default accounts for minors, adjustments to recommender systems, blocking and muting controls, and safety- and privacy-by-design approaches. In the United Kingdom, Ofcom's current child-protection regime requires relevant services to assess risks to children and addresses governance, age assurance, moderation, reporting, recommender systems, settings, and user support.

The UK Information Commissioner's Children's Code centers children's best interests and emphasizes data-minimizing defaults, while the updated U.S. COPPA Rule strengthens requirements concerning children's data, targeted advertising, retention, and biometric identifiers. These developments

indicate a growing shift from parental responsibility alone toward organizational accountability and safer product architecture.

Despite this progress, immersive-child protection remains fragmented across disciplines. Developmental psychology examines children's evolving cognitive and psychosocial capacities; cybersecurity focuses on technical compromise; privacy research evaluates data collection and inference; HCI investigates interaction design; content governance addresses harmful communication; education emphasizes literacy and resilience; and law defines institutional obligations.

Treating these areas separately creates gaps precisely where immersive technologies combine them. The present paper therefore develops an interdisciplinary Child-Centered Immersive Protection Framework that treats safety as a coordinated system. The framework is evaluated through simulated scenarios rather than fabricated empirical observations and is intended to provide a reproducible foundation for subsequent field research, platform audits, experimental studies, and policy evaluation.

2. Objectives of the Study

2.1 To Develop an Interdisciplinary Child-Protection Framework

The first objective is to integrate developmental, technological, social, privacy, educational, and governance perspectives within a common framework for immersive digital environments. Protection is approached as a lifecycle responsibility beginning with product conception and continuing through deployment, monitoring, incident response, and revision.

2.2 To Identify Critical Risk and Safeguard Domains

The second objective is to examine six interconnected dimensions of immersive child safety: developmental appropriateness, safety-by-design, privacy and data minimization, age assurance, moderation and reporting, and child–parent empowerment.

2.3 To Compare Fragmented and Integrated Protection Architectures

The third objective is to evaluate, through an explicitly simulated model, how fragmented reactive safeguards differ conceptually from platform-centered, compliance-led, and fully interdisciplinary child-centered approaches.

3. Review of Literature

3.1 Child Development, Presence, and Embodied Immersion

Children cannot be treated simply as smaller adult users. Their cognitive, emotional, social, and physical capacities develop over time, affecting their ability to understand risk, distinguish persuasive intent, interpret social boundaries, manage privacy, evaluate strangers, and respond appropriately during stressful encounters.

Kaimara, Oikonomou, and Deliyannis reviewed 85 studies concerning VR and children and adolescents across physical, cognitive, and psychosocial domains. Their systematic review concluded that the evidence base contains both opportunities and unresolved ethical and developmental concerns, reinforcing the need for age-sensitive health, safety, and usage considerations.

Immersive environments may influence children differently from conventional screen media because interaction occurs through embodied perspective. Users do not simply watch a character being approached; they may experience another avatar entering their perceived personal space. They do not merely view an environment; they navigate through it using body movement, controllers, gaze, or gestures.

This sense of presence can enhance education, play, creativity, and social engagement. Maloney, Freeman, and Robb's studies of social VR found that children and teenagers use immersive environments for socialization and relationship-building, demonstrating that safety strategies should preserve legitimate opportunities for participation rather than seek to exclude children from digital innovation altogether.

The UN Committee on the Rights of the Child's General Comment No. 25 similarly establishes that children's rights apply within the digital environment. A child-centered protection model must therefore consider protection together with participation, access, privacy, development, and evolving capacities.

This rights-based approach is important because overprotection can also create disadvantages. Restrictive systems that indiscriminately block communication, creativity, education, or peer interaction may reduce children's opportunities without adequately addressing underlying platform risks.

The appropriate question is therefore not whether children should participate in immersive environments, but how immersive environments should be designed so that participation remains developmentally appropriate and rights-respecting.

3.2 Social Interaction, Privacy, Security, and Immersive Harm

Social VR introduces interaction patterns that combine characteristics of online gaming, voice communication, social networks, physical space, and avatar-mediated identity.

Maloney, Freeman, and Robb's work highlighted adult concerns about children's harassment, privacy, exposure to negative environments, and unsupervised interaction in social VR. Zheng and colleagues later analyzed documented social-VR incidents and identified multiple safety risks while examining existing platform safety features. Their work emphasizes the need to rethink safety mechanisms in response to multimodal and embodied interactions rather than simply reproducing conventional social-media tools.

Fiani, O'Hagan, McGill, and Khamis extended this design-oriented approach in 2026 by examining expert considerations for real-time social-VR safety features intended to protect children against individual and group harassment. Their work supports rapid, accessible, child-appropriate intervention mechanisms rather than placing the full burden of managing harmful incidents on young users.

Immersive privacy risks are equally significant. Cao and colleagues found that the VR environment involves sensitive information such as eye and motion tracking and that parents may not fully recognize security and privacy implications. Their participants identified parents, educators, companies, and governments as necessary stakeholders in a broader protective ecosystem.

Guo and colleagues' application-level security study provides a complementary technical perspective. Their assessment of 500 popular VR applications found security vulnerabilities, privacy

leaks, and inconsistencies between application behavior and privacy-policy disclosures. Hine and colleagues likewise argue that immersive extended reality raises distinctive safety and privacy issues and recommend stronger attention to biometric information, governance, harassment, and privacy protection. These risks are not independent. An interaction system may simultaneously expose a child's voice, location cues, movement patterns, social relationships, and behavioral preferences. A harmful user may exploit both interpersonal communication and information disclosed through the platform.

Accordingly, a strong safeguarding architecture must coordinate security, privacy, moderation, identity management, interaction boundaries, and user-support mechanisms.

3.3 Children's Rights, Safety-by-Design, and the Interdisciplinary Gap

International policy is increasingly converging around proactive design rather than purely reactive enforcement.

The OECD's digital safety-by-design work identifies age assurance, child-centered design, prevention and detection of harm, privacy protection, child-friendly information, complaints and redress, child participation, and a culture of safety as important elements of safer digital services.

The European Commission's guidelines on minors under the DSA similarly adopt a rights-based and risk-based approach. Recommendations include private-by-default profiles, safer recommender systems, blocking and muting capabilities, and mechanisms that give children greater control.

The UK's Children's Code represents a complementary privacy-centered approach. Its 15 standards emphasize children's best interests and data-protective defaults while seeking to preserve opportunities to explore and develop online.

Ofcom's current Online Safety Act implementation adds operational requirements involving children's risk assessment, moderation, reporting, recommender systems, age assurance, governance, and user support.

The revised U.S. COPPA Rule strengthens requirements involving third-party disclosure for targeted advertising, data retention, and biometric identifiers within its scope.

Platform governance may detect harmful content but overlook biometric privacy. Privacy engineering may minimize data while overlooking harassment. Age assurance may separate age groups but introduce new privacy risks. Parental controls may provide oversight while becoming ineffective if complicated or technically inaccessible. Literacy programs may improve children's skills but cannot compensate for unsafe platform architecture.

4. Research Methodology

4.1 Research Design and Evidence Integration

The study adopts a simulation-based interdisciplinary framework-development methodology.

No human participants were recruited, no children were observed, and no platform safety incidents were experimentally generated.

The conceptual framework was developed by integrating evidence from five categories:

1. peer-reviewed research on children and social VR;
2. VR security and privacy research;
3. child-development and immersive-technology literature;

4. international child-rights and safety-by-design guidance; and
5. current regulatory approaches addressing children's online safety and privacy.

The framework is not intended to calculate real-world probabilities of child harm. Instead, it provides a structured means of evaluating whether an immersive platform addresses multiple categories of child protection simultaneously.

4.2 Construction of the Child-Centered Immersive Protection Framework

Six domains were selected because they represent distinct but interconnected requirements repeatedly identified across research and policy.

Table 1: Operational Structure of the Child-Centered Immersive Protection Framework

Protection Domain	Core Risk Addressed	Illustrative Safeguards	Evaluation Scale
Developmental Appropriateness	Experiences exceeding children's evolving cognitive, emotional, social, or physical capacities	Age-sensitive interaction design, developmental testing, session guidance, accessible explanations	0–100
Safety-by-Design	Harm being addressed only after exposure	Safe defaults, interaction boundaries, proactive risk assessment, friction against harmful behavior	0–100
Privacy & Data Minimization	Excessive collection or reuse of biometric, behavioral, voice, gaze, movement, and spatial data	Data minimization, local processing, restricted retention, child-protective defaults	0–100
Age Assurance	Children accessing unsuitable spaces or adults entering child-oriented environments without appropriate controls	Proportionate privacy-preserving age assurance and differentiated experiences	0–100
Moderation & Reporting	Harassment, grooming, bullying, harmful content, or abusive social interaction	Real-time reporting, blocking, muting, personal boundaries, trained moderation, escalation	0–100

Source: Author-developed interdisciplinary simulation framework informed by OECD, UNICEF, European Commission, ICO, Ofcom, FTC, eSafety, and peer-reviewed XR safety research.

The framework intentionally avoids assigning safety responsibility exclusively to the child.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

A young user may receive digital-literacy education and still encounter design features that expose them to adults, retain biometric information unnecessarily, or make emergency controls difficult to access.

Similarly, parental supervision is useful but cannot substitute for secure engineering, professional moderation, risk assessment, or appropriate product defaults.

4.3 Simulation Strategy and Ethical Boundaries

Four hypothetical system architectures were constructed:

- Fragmented Reactive Protection: safeguards are added mainly after incidents occur.
- Platform-Centric Protection: technical safety tools exist, but developmental, educational, regulatory, and privacy dimensions remain incompletely integrated.
- Compliance-Led Protection: major regulatory requirements are addressed systematically, although user-centered and developmental integration remains uneven.
- Interdisciplinary Child-Centered Protection: developmental science, privacy engineering, age assurance, moderation, product design, family support, child participation, and governance operate as a coordinated system.
- Scores from 0 to 100 were assigned for methodological demonstration.

A future empirical validation should combine child-centered participatory design, parental interviews, platform audits, incident-response testing, privacy and security assessment, usability studies, moderation-performance analysis, developmental review, and longitudinal safety outcomes.

5. Analysis

5.1 Comparative Performance of Protection Architectures

The simulation illustrates substantial differences between isolated safeguards and integrated protection.

Table 2: Simulated Child-Protection Performance Across Four Architectures

Protection Architecture	Developmental Appropriateness	Safety-by-Design	Privacy & Data Minimization	Age Assurance	Moderation & Reporting	Child–Parent Empowerment	Composite Score
Fragmented Reactive	46	34	37	30	42	44	**39**
Platform-Centric	62	66	58	52	68	60	**61**
Compliance-Led	69	71	76	78	72	65	**72**
Interdisciplinary Child-Centered	89	92	90	86	88	87	**89**

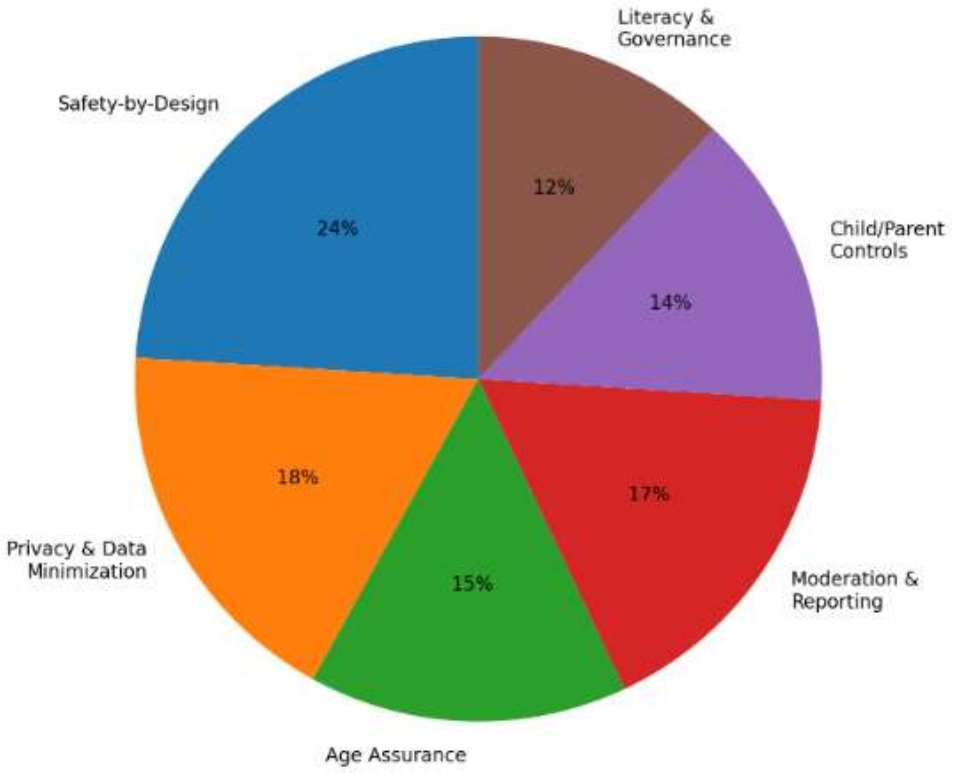
American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Source: Simulated analytical values developed for conceptual comparison. They are not empirical effect estimates.

5.2 Distribution of Protective Capacity

Graph 1: Simulated Protective-Capacity Allocation Across Safeguard Domains



The graph assigns the largest illustrative weighting to safety-by-design at 24%, followed by privacy and data minimization at 18%, moderation and reporting at 17%, age assurance at 15%, child and parent controls at 14%, and literacy and governance at 12%.

Safety-by-design receives the largest share because upstream product architecture determines the conditions under which later safeguards operate. This emphasis aligns with OECD and eSafety approaches that advocate integrating child safety into products and services from the beginning.

Privacy receives substantial weight because immersive systems may generate unusually rich behavioral and biometric information. Empirical VR security research demonstrates why protection must extend beyond conventional account information.

Moderation remains essential because immersive environments permit spontaneous real-time interaction that cannot always be prevented through automated design.

Age assurance is important but intentionally does not dominate the model. Knowing or estimating a user's age does not itself create a safe environment; it must activate age-appropriate defaults and safeguards.

5.3 Interdependence Among Safeguards

The principal analytical finding is that the six dimensions operate multiplicatively in practice even when scored additively in the simulation.

- Consider an immersive world with excellent age assurance but weak moderation.
- Children may be successfully assigned to an age-specific area but still encounter bullying or abuse from other minors.
- Consider a system with strong parental controls but excessive biometric collection.
- The parent may manage social interaction while remaining unable to control complex downstream data uses.
- Consider a platform with sophisticated automated moderation but confusing reporting controls.
- A child experiencing immediate spatial harassment may not know how to activate protection rapidly enough.
- Recent research on real-time safety tools reinforces the need for controls that respond to the immediate and embodied nature of social-VR harassment.

6. Discussion

6.1 Moving Child Protection Upstream

The central implication of this study is that immersive safety should move from incident response to risk prevention.

- Traditional approaches frequently begin after a harmful encounter: a child blocks another user, reports content, informs a parent, or leaves the environment.
- These options remain necessary, but they constitute downstream controls.
- Safety-by-design asks an earlier question:
- What features of the product made the harmful interaction possible or unnecessarily likely?
- For example, unrestricted adult–child contact, public-by-default profiles, unlimited stranger proximity, persistent behavioral tracking, unmoderated voice communication, or recommendation systems that repeatedly direct children toward unsuitable spaces may constitute architecture-level risks.
- The European Commission's DSA guidelines recommend private-by-default accounts for minors, safer recommender approaches, blocking and muting, and safety- and privacy-by-design measures.

6.2 Balancing Age Assurance, Privacy, and Developmental Proportionality

Age assurance is one of the most difficult elements of immersive protection because it solves one problem while potentially creating another.

1. A platform must understand enough about a user to provide an age-appropriate experience.
2. Yet gathering additional identity documents, facial information, biometric characteristics, or behavioral signals may increase privacy risk.
3. The OECD explicitly recommends that age-related restrictions be proportionate, privacy-preserving, and effectively enforced. European child-protection guidance similarly places age assurance within a broader risk-based framework rather than treating it as an end in itself.

4. The design objective should consequently be age-appropriate access with minimal additional information collection.
5. Where exact identity is unnecessary, systems should avoid treating identity verification and age assurance as synonymous.
6. Immersive platforms should also recognize developmental differences within the broad category of "children."
7. A six-year-old, an eleven-year-old, and a sixteen-year-old possess very different capacities, expectations, social needs, and privacy interests.
8. The UK's Children's Code explicitly incorporates age and developmental stages within its design approach.

6.3 Shared Governance, Parental Support, and Child Participation

A further implication is that immersive child safety requires distributed accountability.

- Cao and colleagues found that parents perceived an important role for parents, educators, VR companies, and governments and that technical limitations could restrict practical use of parental controls.
- Parents therefore need understandable tools rather than merely more settings.
- A useful parent dashboard should explain social-contact permissions, purchasing, play duration, reporting history, data categories, privacy settings, and age-related controls in accessible language.
- However, parental tools should not become a substitute for provider responsibility.
- Technology companies control the architecture, data flows, recommendation systems, default settings, moderation infrastructure, and commercial incentives of immersive environments.
- They consequently hold capabilities that families cannot reproduce individually.
- Governments and regulators establish minimum standards and accountability mechanisms, while educators can strengthen children's digital judgment and help them understand immersive social boundaries.

The OECD explicitly includes child participation among the elements of safety-by-design, while the European Commission reports engagement with children and young people in the development of its minors guidelines.

7. Conclusion

Immersive digital worlds represent an important new phase of children's digital participation.

They can support learning, creativity, play, collaboration, identity exploration, communication, and meaningful social connection. UNICEF and child-rights frameworks appropriately caution against responding to emerging risks by excluding children from technological opportunities altogether.

- At the same time, immersive interaction introduces forms of risk that differ materially from traditional screen-based environments.
- Harassment can become spatial and embodied.
- Stranger interaction can occur through real-time voice and gesture.
- Biometric and behavioral information can become integral to system operation.
- Physical and virtual environments can interact.
- Moderation must interpret multimodal and transient incidents.

- Age distinctions can influence both access and social interaction.

Existing research demonstrates that children's immersive experiences involve concerns spanning harassment, inappropriate interaction, privacy, parental awareness, data processing, security, and platform design.

It is one in which foreseeable risks have already been reduced through thoughtful design, minimal data practices, developmentally appropriate experiences, effective intervention tools, accountable institutions, and meaningful respect for children's rights.

References

1. Livingstone, S., Stoilova, M., & Nandagiri, R. (2018). Children's data and privacy online: Growing up in a digital age. *London School of Economics and Political Science*.
2. Livingstone, S., Stoilova, M., & Nandagiri, R. (2018). Children's conception of privacy online. *London School of Economics and Political Science*.
3. Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. *New Media & Society, 19*(5), 657–670.
4. Livingstone, S., Mascheroni, G., & Staksrud, E. (2018). European research on children's internet use: Assessing the past and anticipating the future. *New Media & Society, 20*(3), 1103–1122.
5. UNICEF. (2017). *The State of the World's Children 2017: Children in a Digital World*. UNICEF.
6. International Telecommunication Union. (2020). *Guidelines for Industry on Child Online Protection*. ITU/UNICEF. The guidelines provide a multi-stakeholder basis for safer Internet-based services and technologies for children.
7. OECD. (2019). *Educating 21st Century Children: Emotional Well-Being in the Digital Age*. OECD Publishing.
8. Council of Europe. (2018). *Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment*. Council of Europe.
9. UNICEF. (2019). *Policy Guidance on AI for Children*. UNICEF.
10. Zhao, J., Lyngs, U., & Shadbolt, N. (2018). What privacy concerns do parents have about children's mobile apps, and how can they stay SHARP? *arXiv preprint*. The study examined parental concerns about children's privacy, inappropriate content, advertising and third-party access to children's information.
11. Slater, M., Gonzalez-Liencres, C., Haggard, P., Vinkers, C., Gregory-Clarke, R., Jelley, S., Watson, Z., Breen, G., Schwarz, R., Steptoe, W., Szostak, D., Halan, S., Fox, D., & Silver, J. (2020). The ethics of realism in virtual and augmented reality. *Frontiers in Virtual Reality, 1*, 1.
12. Huang, Z., Zhang, Y., Quigley, K. C., Sankar, R., Wormser, C., Mo, X., & Yang, A. Y. (2019). Accessibility of virtual reality locomotion modalities to adults and minors. *arXiv preprint arXiv:1904.08009*.
13. Araiza-Alba, P., Keane, T., Matthews, B., Simpson, K., Strugnell, G., Chen, W. S., & Kaufman, J. (2020). The potential of 360-degree virtual reality videos to teach water-safety skills to children. *Computers & Education, 146*, 103768.

14. Freeman, D., Reeve, S., Robinson, A., Ehlers, A., Clark, D., Spanlang, B., & Slater, M. (2017). Virtual reality in the assessment, understanding, and treatment of mental health disorders. *Psychological Medicine, 47*(14), 2393–2400.
15. Madary, M., & Metzinger, T. K. (2016). Real virtuality: A code of ethical conduct—Recommendations for good scientific practice and the consumers of VR-technology. *Frontiers in Robotics and AI, 3*, 3.
16. Brey, P. (2014). The physical and social reality of virtual worlds. *The Oxford Handbook of Virtuality*. Oxford University Press.
17. Baek, Y., Kim, M., & Lee, S. (2019). The effects of immersive virtual environments on children's learning and interaction. *Educational Technology research literature*.
18. Wartella, E., Rideout, V., Lauricella, A. R., & Connell, S. L. (2014). Parenting in the age of digital technology: A national survey. *Center on Media and Human Development, Northwestern University*.
19. Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *Risks and Safety on the Internet: The Perspective of European Children*. EU Kids Online, London School of Economics and Political Science.
20. Council of Europe. (2019). *Digital Citizenship Education Handbook: Being Online, Well-Being Online, and Rights Online*. Council of Europe.