

What Parents Should Know to Help Protect their Kids and Youth Online

Risks associated with playing Virtual Reality Games and the Metaverse

Abstract

Risks in VR gaming

- **Inappropriate content:** A “mild” scene in a regular game can feel frightening in VR because it seems real.
- **Online interactions:** Multiplayer VR spaces sometimes connect children with strangers, raising risks of bullying or grooming, and unsafe digital interaction.
- **Purchases:** Immersion can make kids more likely to spend impulsively on “in-game” items.

Information Compiled: 18 January 2026

By: Glen Hutton

for the



Contents

What is VR?	4
Dangers of VR.....	4
Physical Dangers	4
Eye Strain & Vision:	4
Motion Sickness:	4
Injuries:	4
Physical Discomfort:	4
Social & Psychological Dangers	5
Exposure to Harmful Content:	5
Grooming & Exploitation:	5
Blurring Reality:	5
Addiction, Over-Immersion, and Mental Health:	5
Cyberbullying & Harassment:	5
Key Privacy Concerns	5
Biometric & Behavioral Data:.....	5
Inference of Sensitive Info:	5
Data Misuse:	5
Security Vulnerabilities:	6
Social Engineering:	6
Lack of Informed Consent:	6
Deepfakes:	6
Safety & Control Issues	6
Poor Parental Controls:.....	6
Lack of Age Verification:.....	6
Recommendations	6
Restrict Use:	6
Supervise & Limit:.....	6
CHOOSE AGE-APPROPRIATE CONTENT:	6
What is the metaverse?	7
Metaverse	7
What are the risks?	7
Some of the potential areas of concern include:	8

Teens being groomed:.....	8
Being exposed to graphic sexual content:	8
Sexual harassment, cyberbullying, threats of violence, and racism:	8
Often no age verification:	8
Limited parental controls with VR devices:.....	8
Significantly reduced ability for parents to “see” what’s happening:	8
What can parents do?	9
Parental Supervision.....	9

WHAT IS VR?

- VR stands for “virtual reality”. Putting on a wearable console system allows you to see and interact with a 360-degree computer-generated world.
- Inside the headset you’re completely surrounded by whatever virtual content you load up, including surround sound.
- To look at a virtual sky, you look up. If someone shoots a gun behind you, it sounds like it went off behind you.
- Everything in VR feels a lot more real and more intense than on 2-D screens. It’s like you’re inside of a game.

DANGERS OF VR

- Dangers of children playing VR include physical issues (eye strain, dizziness, balance problems, injury from moving blindly) and psychological/social risks like exposure to inappropriate content (violence, sexual themes), cyberbullying, grooming by adults, potential addiction, and difficulty distinguishing fantasy from reality, with many headsets not sized for kids and lacking robust parental controls.
- Major health warnings advise against use for kids under 13 due to developmental concerns.

PHYSICAL DANGERS

EYE STRAIN & VISION:

- VR headsets, designed for adults, can strain developing eyes, potentially causing temporary double vision, blurry vision, or even lazy eye (amblyopia) in younger children.

MOTION SICKNESS:

- Disorientation, dizziness, and nausea are common due to visual-vestibular mismatch.

INJURIES:

- Children can trip, fall, or hit objects in their real-world environment while immersed, leading to broken bones or other physical harm.

PHYSICAL DISCOMFORT:

- Headaches, muscle soreness, or fatigue can occur from improper headset fit or long sessions.

SOCIAL & PSYCHOLOGICAL DANGERS

EXPOSURE TO HARMFUL CONTENT:

- Unmoderated social VR platforms can expose kids to graphic violence, hate speech, cyberbullying, sexual harassment, sexual content, and predatory grooming.

GROOMING & EXPLOITATION:

- Anonymous interactions with adults in immersive spaces increase risks of sexual exploitation, as seen in apps like VRChat and Horizon Worlds.

BLURRING REALITY:

- Highly realistic VR can make it harder for young children to separate game experiences from real life, causing anxiety or a sense of unreality.

ADDICTION, OVER-IMMERSION, AND MENTAL HEALTH:

- Excessive use can lead to dependency, anxiety, and potentially Internet Gaming Disorder.

CYBERBULLYING & HARASSMENT:

- Online multiplayer VR exposes children to interactions with strangers, including cyberbullying

KEY PRIVACY CONCERNS

BIOMETRIC & BEHAVIORAL DATA:

- Eye-tracking reveals focus, hand/finger tracking can expose PINs, and voiceprints, facial geometry, and movement patterns are highly personal.

INFERENCE OF SENSITIVE INFO:

- This data can infer age, gender, location, ethnicity, political views, and even sexual orientation.

DATA MISUSE:

- Advertisers and other third parties can use this detailed data for hyper-targeted ads or to build intimate user profiles.

SECURITY VULNERABILITIES:

- Data breaches can expose this sensitive information, leading to identity theft, impersonation, or unauthorized transactions.

SOCIAL ENGINEERING:

- Immersive environments create new avenues for phishing, misinformation, and manipulating users.

LACK OF INFORMED CONSENT:

- The sheer volume and nature of data collected make truly informed consent difficult, as users often don't grasp the depth of tracking.

DEEPPAKES:

- Exposure to manipulated media can be confusing and manipulative.

SAFETY & CONTROL ISSUES

POOR PARENTAL CONTROLS:

- Many VR platforms lack robust age-gating or content filtering, and parental controls are often limited.

LACK OF AGE VERIFICATION:

- It's easy for children to bypass age restrictions and access adult-oriented apps.

RECOMMENDATIONS

RESTRICT USE:

- Health bodies and experts suggest avoiding VR for children under 13.

SUPERVISE & LIMIT:

- For older children, monitor usage, set time limits, and use available parental controls (like chat restrictions).

CHOOSE AGE-APPROPRIATE CONTENT:

- Select games with strict age ratings and avoid social platforms with unmoderated user-generated content.

WHAT IS THE METAVERSE?

Protecting Children Online: For Immediate Release

- <https://protectchildren.ca/en/press-and-media/news-releases/2022/metaverse#:~:text=What%20are%20the%20risks?,harassment%20and%20grooming%20of%20minors>.

METAVERSE

- Winnipeg, Canada — [Cybertip.ca](#), Canada's tipline for reporting online child sexual abuse and exploitation, is urging parents to be aware of the **metaverse** and the emerging risks that may come along with children and teens being in the largely unrestricted virtual space.
- In the broadest sense, the metaverse is an online, 3D world where people can interact as digital characters just as they would in the real world. It's mainly accessed by using a virtual reality headset, such as Meta™'s (the parent company of Facebook®) Oculus VR® headsets, and downloading virtual and augmented reality apps for games, chatting, or just hanging out.

WHAT ARE THE RISKS?

- In the metaverse children and adults can mix in a predominantly unmoderated world, which increases the risk of tweens/teens being groomed and victimized by those looking to harm and sexually exploit youth.
- There have been multiple articles in the media pointing to the metaverse's safety shortfalls and risks.
 - One [Washington Post reporter](#) stumbled across an apparent nine-year-old who was using their parent's VR to play in the 18+ app Horizon Worlds, while the [Mirror showcased screenshots](#) of a user name "pedo" talking to a girl as they walk her to a private area in the 3D world of VRChat™, a popular social game.
 - A [BBC researcher posing as a 13-year-old](#) even found strip clubs in the app, was shown sex toys, and was approached by numerous adult men.
- In reviewing VRChat, the [Center for Countering Digital Hate](#) found that users, including minors, **are exposed to abusive behaviour every seven minutes**.
 - The group identified 100 potential violations of Meta's policies for VR, however only 51 met the criteria for reporting offending content.
 - As of when the Center published its findings, Meta had not responded to any of the reports of abusive behaviour, including sexual harassment and grooming of minors.

SOME OF THE POTENTIAL AREAS OF CONCERN INCLUDE:

TEENS BEING GROOMED:

- Conversations within the metaverse could lead to youth being exploited in the app (e.g., committing virtual sex acts or engaging in sexualized chat).
- Or conversations that start in the metaverse, could lead to teens being moved to other platforms—ones that may have a video chat or livestream component—which increases the risk of exploitation.

BEING EXPOSED TO GRAPHIC SEXUAL CONTENT:

- For example, the Mirror article outlines a room in VRChat where users—including apparent children—were crowded around a SpongeBob SquarePants avatar as he pretended to commit sex acts.

SEXUAL HARASSMENT, CYBERBULLYING, THREATS OF VIOLENCE, AND RACISM:

- Unlike other platforms, there are often no content filters, and many apps within the metaverse rely on users to regulate their own experience, muting, blocking, or reporting users.

OFTEN NO AGE VERIFICATION:

- For example, Meta’s safety page states, “While we know that children under 13 may want to use Oculus devices, we do not permit them to create accounts or use Oculus devices.”[1](#)
- However, no age verification is required. Instead, the company relies on users’ Facebook accounts to use an Oculus device.
- This minor hurdle can easily be bypassed by a child using a shared family device or Facebook account.

LIMITED PARENTAL CONTROLS WITH VR DEVICES:

- Meta’s Oculus Quest 2 headset doesn’t currently come with the option to turn on parent controls that help to limit access to 18+ or otherwise harmful content (although parents can restrict specific sites through the settings for the web browser on the device).[2](#)
- Other companies are adding options. HTC® recently rolled out Vive Guardian app, which allows users to limit app and content access within Vive® VR devices, as well as pushing requests for downloads.

SIGNIFICANTLY REDUCED ABILITY FOR PARENTS TO “SEE” WHAT’S HAPPENING:

- With other video games, parents can watch what’s happening on screen, but with a VR/AR device, where all the activity is self-contained, parents can be in the dark about what’s occurring in the metaverse.

- A few systems, like Quest® and Vive, allow for what’s happening within the device to be “cast” to a phone, tablet, or smart TV, leaving parents and teens to work together on rules around providing visual access.

WHAT CAN PARENTS DO?

PARENTAL SUPERVISION

Cybertip.ca recommends a high level of parental supervision and monitoring when their children use metaverse due to the situations they may encounter.

- The metaverse is not intended for children under the age of 13.
- If you have a VR/AR device, take care that your child does not have access to it. Consider signing out of your account.
- Learn about the metaverse, the VR/AR devices, and the games/apps your teen is interested in playing.
 - Does the game/app have any form of privacy controls (e.g., can you limit who your teen plays with or chats with)?
 - Are there options to report inappropriate activity?
 - Does the game/app connect to other platforms/apps/sites outside the metaverse?
- Remind your teen that not everyone in the metaverse is who they say they are.
 - Just because the person’s avatar appears as a peer, doesn’t mean they actually are.
- Have regular conversations about what they are doing in the metaverse and who they are playing/chatting with.
 - Know your teen’s passwords, screen names, and the people they are playing with.
- Discuss how to get out of uncomfortable situations.
 - Due to the immersive nature of the metaverse, it may be harder for teens to “walk” away from a situation or conversation.
 - Reinforce with your teen that you understand how quickly it is possible to encounter an inappropriate or problematic situation and you are the right person to go to if they need help or are upset.
 - Remind them that you want to know so you can support and help them.
- Talk with your teen about the risks associated with metaverse, how they can reduce these risks, and what to do if something happens.
 - Ensure your teen understands they can talk to you about anything they encounter that makes them feel uncomfortable without fear of losing phone or gaming privileges.

If you see or read anything sexual towards your children online, report it to [Cybertip.ca](https://www.cybertip.ca) or your local law enforcement agency.