



Ethical Considerations

CHAPTER 7

M-STEM

PROJECT NUMBER: 2023-1-FR01-KA220-SCH-000151516



Co-funded by
the European Union



Colegio
Séneca
S.Coop.And



AGRUPAMENTO DE
ESCOLAS DE BARCELOS
EDUCAÇÃO PÚBLICA DE QUALIDADE



EURASIA INSTITUTE



INSPECTORATUL ȘCOLAR
JUDEȚEAN TELEORMAN



City of Malmö



Introduction

The educational field is being overtaken by the metaverse, which will alter methods of human-computer interaction. Given the speed at which technology is advancing, prominent tech CEOs are coming up with creative methods to make the Metaverse a learning environment. People have become used to telemedicine, teleworking, and many other types of remote communication since the COVID-19 pandemic. Many educators have been concentrating on the Metaverse lately. Following Facebook's announcement that it was renaming and marketing itself as Meta, moreover interest in computer science and education increased. Exciting new approaches to student engagement, collaborative learning, real-world simulation, and personalized experiences are provided via metaverse tools. However, there are a number of ethical issues that arise with increased immersion and data collecting that educators need to be aware of and deal with an emphasis on privacy, security, and responsible practice, We must also take into account a number of ethical concerns as the virtual environment grows more intricate and potentially intrusive, including data privacy and security, digital identity, equity and access, ownership, and control of the influence of immersive technology on intellectual property. This chapter examines the main ethical issues surrounding the use of technology and the Metaverse in education. Additionally, it offers instructors helpful advice on how to handle possible difficulties in the classroom, address inquiries from students, and include Metaverse experiences in ways that are respectful, safe, and consistent with educational ideals.

Ethical Considerations in the Metaverse

Privacy and Data Protection

The Metaverse and AI platforms relies on tracking a wide range of user information, including:

- Personal profile data - Name, email, social media accounts , pictures and video files
- Behavioral data - Interactions, choices, movement patterns, search history
- Biometric or sensor data - VR/AR equipment

Key Ethical Issues:

- Informed Consent: Learners must understand what data is being collected and how it will be used. This includes explicit permission from parents for minors.
- Data Minimisation: Only essential data should be collected and stored.
- Third-Party Sharing: Many Metaverse platforms share data with external partners. Schools and educators must be transparent about this and, where possible, choose platforms with strong privacy commitments.



Co-funded by
the European Union



Colegio
Séneca
S.CoopAnd

AGRUPAMENTO DE
ESCOLAS DE BARCELOS
EDUCAÇÃO PÚBLICA DE QUALIDADE



INSPECTORATUL ȘCOLAR
JUDEȚEAN TELEORMĂN



Security in Virtual Environments



Major Security Concerns and Solutions

Security isn't just about passwords it includes protecting users from digital harms that may arise in immersive spaces.

1) Malware (Viruses, Trojans, Ransomware)

Malware refers to malicious software designed to damage systems, steal data, or block access to devices. Ransomware, for example, locks files and demands payment for their release.

Solutions

- Install reliable antivirus and anti-malware software
- Keep operating systems and applications regularly updated
- Avoid downloading files from unknown or untrusted sources
- Perform regular data backups



Co-funded by
the European Union



Colegio
Séneca
S.CoopAnd

AGRUPAMENTO DE
ESCOLAS DE BARCELÓS
EDUCAÇÃO PÚBLICA DE QUALIDADE



INSPECTORATUL ȘCOLAR
JUDEȚEAN TELEORMAN



2) Phishing and Social Engineering Attacks

Phishing attacks trick users into revealing sensitive information (passwords, bank details) through fake emails, messages, or websites. Social engineering exploits human trust rather than technical flaws.

Solutions

- Educate users to recognize suspicious emails and links
- Verify sender identity before clicking or responding
- Use email filtering and spam protection
- Enable multi-factor authentication (MFA)



Co-funded by
the European Union



3) Data Breaches and Privacy Violations

Unauthorized access to personal, institutional, or financial data can result in identity theft, financial loss, and reputational damage.

Solutions

- Encrypt sensitive data (both in storage and during transmission)
- Limit data access based on user roles (least-privilege principle)
- Comply with data protection regulations (e.g., GDPR)
- Monitor systems for unusual activity

Security Concern	Key Solution
Malware	Antivirus, updates, backups
Phishing	Awareness, MFA, email filters
Weak passwords	Strong passwords, password managers
Data breaches	Encryption, access control
Insecure networks	VPNs, secure Wi-Fi
Cyberbullying	Policies, moderation, education
Identity theft	Privacy controls, monitoring
Outdated software	Regular updates



Co-funded by
the European Union

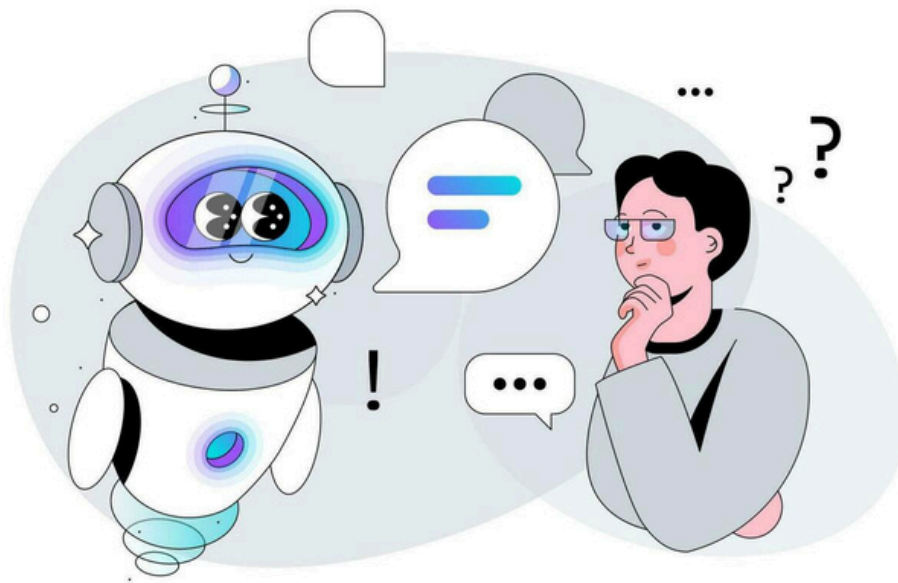


Guidelines and Responsible Practices

Educators should be aware of laws that apply when students use digital platforms

- Establish community agreements on acceptable behaviour.
- Use strong authentication (complex passwords, multi-factor authentication).
- Ensure platforms support encrypted communication.
- Monitor “public area” interactions with trained moderators.
- Have classroom rules and escalation paths for unsafe behaviour.

Relevant Questions



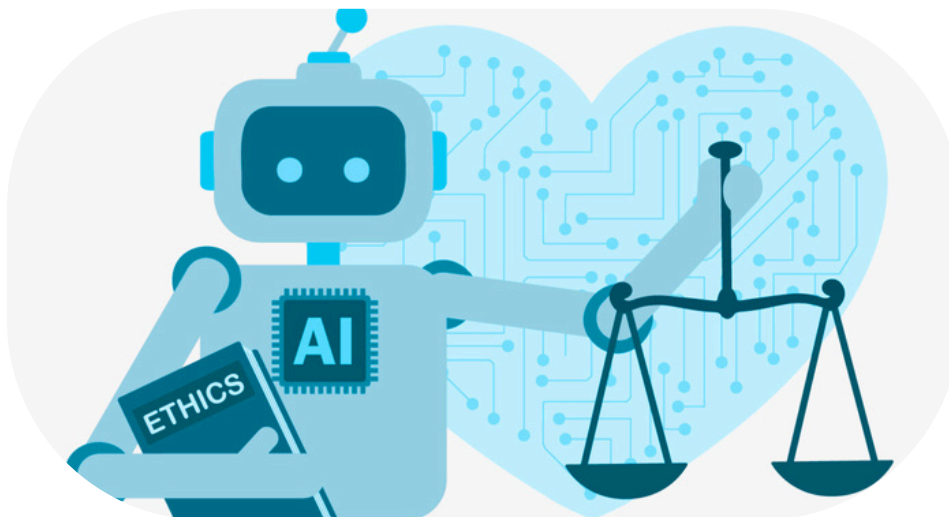
Co-funded by
the European Union



- 1) What data does this Metaverse platform collect, and who can see it? is it possible to hack our class session in the Metaverse?
- 2) How can teachers protect students privacy when using Metaverse and immersive digital platforms in education?
- 3) How can teachers promote responsible and ethical behaviour among students in the Metaverse and other virtual environments?

Ethical Practices in the Metaverse and AI

- Collection of only necessary data
- Ensure informed consent, especially for minors
- Allow users to access, correct, or delete their data
- Transparency and Explainability
- Equality and non discrimination
- Human oversight



Co-funded by
the European Union



Colegio
Séneca
S.CoopAnd

AGRUPAMENTO DE
ESCOLAS DE BARCELÓS
EDUCAÇÃO PÚBLICA DE QUALIDADE



INSPECTORATUL ȘCOLAR
JUDEȚEAN TELEORMĂN



Conclusion

The Metaverse has the potential to revolutionize education through deeper simulations, more participation, and new forms of teamwork. However, this potential needs to be accompanied by a dedication to moral behavior. In order to safeguard digital interactions, promote respectful communities, and preserve privacy, responsible educators adopt preemptive measures. An essential component of responsible and successful learning design is the ethical use of technology and the Metaverse. As the educational landscape becomes more integrated with the Metaverse, a number of significant hazards and concerns become apparent. Data security and privacy are the main concerns. Sensitive student data is more likely to be compromised or exploited as educational interactions become more pervasive and integrated throughout the Metaverse.



Co-funded by
the European Union



References

Kaddoura, S. and Al Hussein, F., 2023. The rising trend of Metaverse in education: Challenges, opportunities, and ethical considerations. PeerJ Computer Science, 9, p.e1252.

ZAMFIR, M., MARINESCU, I.A., IORDACHE, D., BARBU, M. and CÎRNU, C.E., 2023. Exploring ethical considerations in Metaverse from the education perspective. ON VIRTUAL LEARNING-ICVL 2023, p.91.



Co-funded by
the European Union

