

The use of Technology in Education Presents both challenges and Opportunities for Teacher Trainees in a Global Context

Dr. Sujeewa Polgampala ¹, Dr. Anjum Bano ²

Abstract: Technology can inadvertently intensify existing inequalities, enhancing learning and teaching experiences and bringing its own set of complexities. One of the noteworthy challenges in many parts of the world is the lack of a satisfactory level of technological infrastructure and internet access. Without reliable connectivity and access to devices, teachers and students may struggle to fully leverage the benefits of technology in the classroom, though having incorporating technology effectively requires teachers to possess the necessary skills and knowledge to use various digital tools and platforms. Surveys and questionnaires to gather data on teachers access to technology, their proficiency levels, and their experiences with digital tools were distributed among 200 teacher trainees at a reputed national college of teacher education and 30 interviews with educators, policymakers, and students to gain qualitative insights into the challenges and opportunities of technology integration in Sri Lanka. However, 78% of teacher trainees are comfortable or proficient in using technology, which may assist their ability to incorporate it into their teaching practices.

Keywords: *technology, teaching practices, constraints*

Introduction

Since all students do not have equal access to devices, it can create disparities and limit opportunities among students who lack access to technology, resulting in an unfair learning environment (Moore, R., Vitale, D., & Stawinoga, N. 2018). Integrating technology requires a shift in delivery approaches. Adjusting to new pedagogical approaches and finding the right balance between traditional and technology-mediated teaching can be a significant challenge (Okoye, K., Rodriguez-Tort, J. A., Escamilla, J., & Hosseini, S. 2021).

Integrating technology in education can make learning more interactive and engaging for students through multimedia presentations, gamified learning platforms, virtual simulations, and educational apps can increase student motivation and make complex concepts more accessible and enjoyable (Suleyman, M. 2023). To address the challenges and fully embrace the opportunities, teachers need support and professional development opportunities. Schools, districts, and educational institutions should invest in training programs to equip teachers with the necessary technological skills, pedagogical knowledge, and strategies to integrate technology effectively. Additionally, efforts should be made to bridge the digital divide and ensure equitable access to

¹ Cinec Campus, Malabe, Sri Lanka, Sujeewa.polgampala@cinec.edu

² Iqra University, Pakistan, Anjum.bano@iuk.edu.pk

technology for all students, irrespective of their socioeconomic backgrounds. Cyber harassment among school children has become a pressing issue in today's digital age. The harmful effects of online bullying and harassment can have long-lasting consequences on the mental health, self-esteem, and academic performance of young individuals. To address this critical problem, this proposal introduces "SafeSpace," an innovative solution that aims to prevent cyber harassment and create a safe and supportive digital environment for school children.

Literature Related to the Use of Technology in the Learning and Teaching Process

The use of technology in education has become increasingly prevalent and impactful in recent years. It has revolutionized the way students learn and has opened up new avenues for teaching and collaboration (**Kissinger, H. et al., 2021**). Technology has played a crucial role in enabling remote learning, especially during the COVID-19 pandemic. Virtual classrooms, video conferencing, and online learning platforms have allowed students to continue their education from home, ensuring continuity of learning during challenging times (**Fabry, D. L. et al., 1997**). Here are some key aspects and benefits of technology in education. Technology provides students and educators with instant access to a vast amount of information and resources. The internet, online libraries, and educational platforms allow learners to explore various topics, conduct research, and access up-to-date information from anywhere at any time (**Anyim, W. O. 2021**). and also offer interactive learning experiences through multimedia elements, such as videos, simulations, and virtual reality (VR) applications. These tools engage students and make the learning process more immersive and dynamic (**Brynjolfsson, E. et al., 2020**). catering to different learning styles. With technology, educators can personalize instruction based on individual student needs. Adaptive learning systems and intelligent tutoring systems analyze student performance and provide personalized recommendations and feedback, helping students progress at their own pace. Moreover, it enables collaboration among students and educators across different locations. Online platforms, discussion forums, and video conferencing tools facilitate communication, allowing students to collaborate on projects, share ideas, and receive feedback from peers and expert processes (**Mishna, F et al., 2010**). Technology offers various assessment tools, including online quizzes, interactive assignments, and automated grading systems (Messer, M., Brown, N. C., Kölling, M., & Shi, M. 2024). These tools streamline the assessment process, provide immediate feedback to students, and generate data for educators to track student progress and identify areas for improvement. Technology has connected students and educators worldwide, opening up opportunities for global collaboration and cultural exchange (**Broussard, M. 2023**). Virtual exchange programs, online language learning platforms, and video conferencing tools facilitate cross-cultural learning experiences and promote global awareness. Technology has made education more accessible and inclusive for students with disabilities. Assistive technologies, such as screen readers, speech recognition software, and captioning tools, enable students with disabilities to access educational materials and participate fully in the learning.

Cyber Harassment in Using Technology in Learning and Teaching

While technology has brought numerous benefits to education, it has also given rise to new challenges and risks, including cyber harassment. Cyber harassment refers to the use of digital technology to harass, intimidate, or threaten individuals. In the context of education, it can manifest in various ways, such as cyberbullying by using technology to harass, humiliate, or target their peers. This can occur through social media platforms, messaging apps, or online forums. Cyberbullying can have serious emotional and psychological consequences for the victims, leading to decreased academic performance and a hostile learning environment. Students and educators may encounter harassment from unknown individuals online. This can include receiving abusive messages, threats, or inappropriate content through email, social media, or other communication channels. Online predators can also target students, posing a significant risk to their safety.

Users may face unwanted contact or advances from individuals within their educational community. This can involve persistent messaging, unwanted friend requests, or the sharing of personal information without consent. It is essential to establish and enforce clear boundaries for communication within educational settings. The use of technology in education may involve the collection and sharing of personal information. If not adequately protected, this information can be misused, leading to privacy breaches and potential harassment or identity theft. Safeguarding personal data is crucial to preventing cyber harassment.

Addressing Cyber Harassment in Education

Educational institutions should develop comprehensive policies and guidelines that address cyber harassment. These policies should define acceptable online behavior, outline consequences for harassment, and provide procedures for reporting incidents. Awareness and education about cyber harassment are crucial. Students and educators should be educated on responsible digital citizenship, safe online practices, and the impact of cyber harassment. This includes teaching empathy, respect, and proper online communication etiquette. Creating a safe and supportive learning environment is essential to combat cyber harassment. Encourage open communication and provide channels for reporting incidents. Implement mechanisms for anonymous reporting to protect victims who fear retaliation. Educational institutions should implement robust cybersecurity measures to protect the privacy and security of students and educators. This includes secure online platforms, encryption of sensitive data, strong password policies, and regular system updates. Engage parents and guardians in addressing cyber harassment. Educate them about the risks, signs, and prevention strategies. **(Pasquale F.2020)**. Encourage open communication between parents and educators to address incidents promptly and collaboratively while offering counseling and support services to victims of cyber harassment. Ensure that students and educators have access to resources and guidance to cope with the emotional and psychological effects of cyber harassment.

Cyber Security in Using Technology in Education

Cybersecurity is of paramount importance when using technology in education to protect sensitive data, ensure the privacy of students and educators, and maintain the integrity of digital systems.

Here are some key considerations for implementing cybersecurity measures in educational contexts since safeguarding personal and sensitive data is crucial. Educational institutions should establish robust data protection policies, including encryption of data, access controls, and secure storage practices. Regular data backups should be performed to prevent data loss. Implementing strong user authentication mechanisms, such as complex passwords or two-factor authentication, to prevent unauthorized access to educational systems and resources. Regularly review and update user access permissions to ensure that individuals only have access to the necessary resources. While securing the educational network infrastructure by implementing firewalls, intrusion detection and prevention systems, and regularly updated antivirus software. Regularly patch and update network devices to address known vulnerabilities. It is essential to have reliable and secure online platforms and tools for educational purposes. Ensure that these platforms have robust security features, encryption protocols, and privacy settings to protect the data and communications of students and educators (**Beran, T., & Li, Q. 2005**). Educate students and educators about phishing attacks, which are attempts to trick individuals into revealing sensitive information. Teach them to recognize phishing emails, suspicious links, and attachments and to report any suspicious activity while keeping all software, including operating systems, applications, and plug-ins, up to date with the latest security patches (**Beran, T. et al., 2005**). Regularly update and patch educational systems to address vulnerabilities that attackers could exploit. Implement cybersecurity training and awareness programs to educate students and educators on common security risks (Suleyman, M., et al., 2023), best practices for online safety, and strategies for identifying and responding to potential cybersecurity threats. Establish clear procedures for reporting and managing cybersecurity incidents, and encourage students and educators to promptly report any suspicious activity or security breaches. Develop an incident response plan to address and mitigate the impact of cybersecurity incidents. Ensuring compliance with applicable data protection regulations, such as the General Data Protection Regulation (GDPR) or the Family Educational Rights and Privacy Act (FERPA). Obtain proper consent for data collection and usage, and implement privacy settings that allow individuals to control their personal information. Getting the support of cybersecurity experts, organizations, and industry partners to stay updated on emerging threats and best practices. Collaborate with other educational institutions to share experiences, resources, and strategies for enhancing cybersecurity in education. By implementing these cybersecurity measures, educational institutions can create a safer digital environment, protect sensitive data, and mitigate the risks associated with using technology in education. Regular assessment and improvement of security practices should be an ongoing process to stay ahead of evolving cyber threats.

Use Technology to Minimize Cyber Harassment and Bullying?

While technology can be a platform for cyber harassment and bullying, it can also be harnessed to minimize and prevent such incidents. Here are some ways technology can be used to address cyber harassment and bullying. Technology can be utilized to provide comprehensive online safety education to students. Educational institutions can incorporate digital literacy and responsible online behavior into the curriculum. Teach students about the potential risks and consequences of cyberbullying (**Pruksachatkun, Y. et al., 2023**), how to identify and report cyber harassment, and

strategies to stay safe online. Implement anonymous reporting systems that allow students to report incidents of cyberbullying or harassment without fear of retaliation. Provide clear channels for reporting, ensuring the confidentiality of the individual reporting. This encourages students to come forward and facilitates early intervention. Employ monitoring and filtering tools that can identify and block inappropriate or harmful content. These tools can flag and alert administrators about potential instances of cyberbullying or harassment, enabling timely intervention and support. Encourage social media platforms, online communities, and educational platforms to enforce strong policies against cyberbullying and harassment. These policies should define unacceptable behavior, provide reporting mechanisms, and outline consequences for offenders. Collaborate with platform providers to ensure the safety and well-being of users (**Shariff, S. 2008**).

Leveraging artificial intelligence (**AI**) and natural language processing (**NLP**) technologies to detect and analyze online content for signs of cyberbullying or harassment. AI algorithms can identify harmful language patterns, offensive comments, or threatening messages, alerting administrators to potential incidents. Utilize technology to promote positive online culture and digital citizenship. Launch awareness campaigns that encourage empathy, respect, and kindness in online interactions (**West, D. M. 2020**). Create engaging content, videos, and social media campaigns to spread positive messaging and foster a supportive online environment. Develop or recommend parental control apps and tools that allow parents/guardians to monitor their child's online activities, set appropriate restrictions, and receive notifications about potential cyberbullying incidents. These tools can facilitate parental involvement and early intervention. Fostering a supportive peer network by introducing reporting apps or platforms where students can anonymously report incidents, seek advice, or support each other. Encourage students to look out for their peers and promote a culture of reporting and intervening against cyberbullying. Encourage collaborative online projects and group activities that promote teamwork and positive online interactions. Providing opportunities for students to work together, share ideas, and learn from one another it helps foster a sense of community and reduces the likelihood of cyberbullying incidents.

Responsibility of Educationists to Stop Cyber Bullying

Educationists have to play a crucial role in preventing and addressing cyberbullying. They have a responsibility to create a safe and supportive learning environment for their students. Here are some key responsibilities that educationists have in stopping cyberbullying. Educationists should raise awareness among students about cyberbullying, its consequences, and the importance of respectful online behavior. They should educate students about responsible digital citizenship, empathy, and the impact their online actions can have on others. Educationists should work with their institutions to develop and enforce clear policies that explicitly address cyberbullying. (**Pruksachatkun, Y., et al., 2023**) These policies should define cyberbullying, provide examples of prohibited behavior, and outline consequences for perpetrators. Ensure that these policies are communicated to students, parents, and staff members. Educationists should foster a classroom culture where students feel safe and supported. Promote open communication, respect, and empathy among students. Encourage students to speak up if they witness or experience cyberbullying and assure them that their concerns will be taken seriously. Educationists should

integrate digital literacy into their curriculum, teaching students critical thinking skills, online safety, and responsible use of technology (Suleyman, **M.**, & **Bhaskar, M.**, 2023). Teach students how to navigate the online world, identify and respond to cyberbullying, and develop resilience to cope with online negativity. Educationists should stay vigilant and monitor students' online activities to detect signs of cyberbullying. Promptly address any incidents or reports of cyberbullying by investigating the matter, providing support to the victim, and taking appropriate disciplinary or remedial actions against the perpetrator (**Vandebosch, H.**, et al., 2009).

Educationists should maintain open lines of communication with parents and guardians. Inform them about the school's policies and procedures regarding cyberbullying and seek their support in promoting a safe online environment. Encourage parents to monitor their child's online activities and report any incidents. Educationists should offer support to students who have been victims of cyberbullying. Provide counseling services, encourage peer support, and help victims build resilience. Collaborate with support staff, psychologists, or external resources to provide appropriate interventions for both victims and perpetrators. Educationists should engage in professional development programs to enhance their understanding of cyberbullying, digital safety, and intervention strategies. Stay updated on current trends and research related to cyberbullying to effectively address the issue. By taking these responsibilities seriously, educationists can create a positive learning environment that empowers students to use technology responsibly and prevents the harmful effects of cyberbullying. (**Pasquale, F.** 2020) Collaboration with students, parents, and the wider school community is key to effectively stopping cyberbullying and promoting a culture of respect and kindness both online and offline. It is important to implement a multi-faceted approach that combines technology tools, education, awareness, and strong policies to minimize cyber harassment and bullying. A holistic effort involving students, parents, educators, and technology providers can contribute to creating a safer online environment for all. However, it is important to note that the integration of technology in education should be done thoughtfully and purposefully (**Efthymiopoulos, M. P.**, 2019). It requires adequate infrastructure, teacher training, and consideration of privacy and security concerns. Technology should be used as a tool to enhance teaching and learning, complementing traditional pedagogical approaches rather than replacing them entirely.

Necessity of Cyber Security Policies

Cybersecurity policies are essential for educational institutions to establish clear guidelines, procedures, and standards to protect sensitive data, prevent cyber threats, and promote a secure digital environment (**Davenport, T. H.**, et al., 2023). While the specific details of cybersecurity policies may vary depending on the institution's needs and resources, here are some common elements that should be considered: Clearly define the objectives and scope of the cybersecurity policy. State the purpose, goals, and intended audience of the policy, specifying its applicability to all users within the educational institution. Having clearly defined the roles and responsibilities of individuals involved in cybersecurity, including administrators, IT staff, educators, and students. Outline their responsibilities in safeguarding data, reporting incidents, and following cybersecurity best practices (**Kissinger, H. A.** et al., 2021). Safe Space offers a crucial and timely

solution to the issue of cyber harassment among school children. It is suggested to emphasize awareness, empowerment, and community involvement which can effectively create a safer online environment for students. Cybersecurity policies are essential for organizations and individuals to protect sensitive data, maintaining the integrity of information systems. In conclusion, cybersecurity policies are vital for protecting data, ensuring legal compliance, maintaining business continuity, and managing risks in today's digital world. Without them, organizations and individuals are vulnerable to cyber-attacks, data breaches, and financial losses.

Data Analysis

Surveys from 200 teacher trainees (from a national college of education), and 30 interviews with educators, policymakers, and students were carried out and analyzed using statistical analysis to identify correlations between access to technology, teacher proficiency, and student outcomes. Thematic analysis of interview transcripts to uncover recurring challenges and successful stories. Contrasting results from regions with high and low technological infrastructure to highlight disparities.

Results and Discussion

It was found that 78% of teacher trainees surveyed feel comfortable/proficient in using technology, suggesting a strong foundational skill level. However, 22% may lack confidence, potentially affecting their ability to integrate tech effectively. A significant correlation between reliable internet access and improved student engagement and performance of teachers was researched and it has a positive impact. Analysis of Discrepancies and Insights showed that High self-reported proficiency (78%) vs. infrastructure barriers. Teachers with higher digital literacy levels were more likely to effectively integrate technology into their teaching practices. Students and teachers in underserved areas face substantial barriers, such as limited access to devices and unreliable connectivity, which hinder the adoption of technology in education. Technology can widen existing inequalities due to disparities in infrastructure (e.g., internet access, devices). In Sri Lanka, lack of reliable connectivity and devices hinders effective integration in classrooms.

Conclusion

Challenges identified in infrastructure gaps such as uneven access to devices/connectivity. It was highlighted that even proficient teachers may require pedagogical upskilling for tech integration. Potential mismatches between policy goals and on-ground realities were diagnosed. However, its integration is not without challenges. In many parts of the world, technological infrastructure and internet access remain inadequate, exacerbating existing inequalities. Additionally, the effective use of technology in education requires teachers to possess specific skills and knowledge, which is not always the case. This discussion explores these challenges and their implications for educational equity and effectiveness. While technology holds immense potential to enhance learning and teaching experiences, its benefits are not evenly distributed. Addressing the challenges of infrastructure, access, and teacher preparedness is crucial to ensuring that technology

serves as a tool for equity rather than a source of further inequality. By investing in these areas, stakeholders can create a more inclusive and effective educational landscape.

References

- Anyim, W. O. (2021). Relevance of electronic resources and improvement of access for effective distance learning and continuing education programme. *International Journal of Asian Education*, 2(1), 52–63.
- Beran, T., & Li, Q. (2005). Cyber-harassment: A study of a new method for old behavior. *Journal of Educational Computing Research*, 32(3), 265–284.
- Brown, K., Jackson, M., & Cassidy, W. (2006). Cyber-bullying: Developing policy to direct responses that are equitable and effective in addressing this special form of bullying. *Canadian Journal of Educational Administration and Policy*, (57).
- Broussard, M. (2023). *More than a glitch: Confronting race, gender, and ability bias in tech*. MIT Press.
- Brynjolfsson, E., & McAfee, A. (2020). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. W.W. Norton & Company.
- Davenport, T. H., & Miller, S. M. (2023). *Working with AI: Real stories of human-machine collaboration*. MIT Press.
- Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense, and innovation at NATO. *Journal of Innovation and Entrepreneurship*, 8(1), 1–26.
- Fabry, D. L., & Higgs, J. R. (1997). Barriers to the effective use of technology in education: Current status. *Journal of Educational Computing Research*, 17(4), 385–395. <https://doi.org/10.2190/c770-awa1-cmqr-ytyv>
- Kissinger, H. A., Schmidt, E., & Huttenlocher, D. (2021). *The age of AI: And our human future*. Little, Brown and Company.
- Messer, M., Brown, N. C., Kölling, M., & Shi, M. (2024). Automated grading and feedback tools for programming education: A systematic review. *ACM Transactions on Computing Education*, 24(1), 1–43.
- Mishna, F., Cook, C., Gadalla, T., Daciuk, J., & Solomon, S. (2010). Cyber bullying behaviors among middle and high school students. *American Journal of Orthopsychiatry*, 80(3), 362–374.
- Moore, R., Vitale, D., & Stawinoga, N. (2018). *The digital divide and educational equity: A look at students with very limited access to electronic devices at home*. Insights in Education and Work. ACT, Inc.
- Okoye, K., Rodriguez-Tort, J. A., Escamilla, J., & Hosseini, S. (2021). Technology-mediated teaching and learning process: A conceptual study of educators' response amidst the Covid-19 pandemic. *Education and Information Technologies*, 26, 7225–7257.
- Pasquale, F. (2020). *New laws of robotics: Defending human expertise in the age of AI*. Harvard University Press.
- Pruksachatkun, Y., Mcateer, M., & Majumdar, S. (2023). *Practicing trustworthy machine learning*. O'Reilly Media.

- Shariff, S. (2008). *Cyber-bullying: Issues and solutions for the school, the classroom and the home*. Routledge.
- Suleyman, M., & Bhaskar, M. (2023). *The coming wave: Technology, power, and the twenty-first century's greatest dilemma*. Crown Publishing Group.
- Vandebosch, H., & Van Cleemput, K. (2009). Cyberbullying among youngsters: Profiles of bullies and victims. *New Media & Society*, 11(8), 1349–1371.
- West, D. M. (2020). *The future of work: Robots, AI, and automation*. Brookings Institution Press.