

Digital Ethics during Pandemic AMID Online Education and Learning

Kanala Kiranmayi

Assistant Professor, Department of Computer Applications,
East Point College of Higher Education,
Bengaluru, Karnataka, India
kiranmayi@gmail.com



Publication History

Manuscript Reference No: IJIRAE/RS/Vol.12/Issue12/DCAE10083

Research Article | Open Access | Double-Blind Peer-Reviewed | Article ID: IJIRAE/RS/Vol.12/Issue12/DCAE10083

Received:20, November 2025, Revised:29, November 2025, Accepted: 01, December 2025, Published Online:12, December 2025. <https://www.ijirae.com/volumes/Vol12/iss-12/04.DCAE10083.pdf>

Article Citation: Kanala(2025), Digital Ethics during Pandemic AMID Online Education and Learning, IJIRAE: International Journal of Innovative Research in Advanced Engineering, Volume 12, Issue 12 of 2025 pages 716-720

Doi> <https://doi.org/10.26562/ijirae.2025.v1212.04>

BibTeX Key: Kanala@2025Digital

IJIRAE papers should be cited as IJIRAE (International Journal of Innovative Research in Advanced Engineering, AM Publications, India 2025, ISSN 2349-2163, <https://doi.org/10.26562/ijirae.2025.v1212.04> The journal's official abbreviation is IJIRAE. **Orcid:** <https://orcid.org/0009-0004-9398-7488>

Copyright©2025 copyright by the authors. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Abstract: Digital technologies are currently creating both opportunities and potential obstacles with significant ethical implications that will play out over the next few decades. During COVID-Lockdowns, digital technology can be used to boost learning and communication across a range of domains and boundaries. In the worst-case scenario, digital technologies create new divides between those who have access to them and those who do not, raising concerns about surveillance. The real-time disruption of educational environments, systems, participants, and stakeholders caused by COVID-19 is still going on. The Internet of Things is predicted to make a significant impact, particularly during a pandemic. Using IoT services during pandemics has a number of advantages, the most important of which is that they help to keep people physically apart from one another. However, the biggest challenge people face is that the use of the IoT increases social distance and decreases personal communication.

Keywords: IoT, Digital Ethics, Data Privacy, Data Protection, Human Dignity.

I. INTRODUCTION

The Internet of Things (IoT) is a new way of thinking about how new technologies can be applied in the IT industry. The term "Internet of Things" is made up of two words: "internet" and "things." It's a term that refers to the interconnection of devices and machines across the internet. The internet is a worldwide network of interconnected computer networks that use Internet Protocols (IPs) and Transmission Control Protocols (TCPs) to provide services to billions of users. The internet of things (IoT) is a rapidly expanding sector of technology that refers to the interconnection of physical objects. The internet of things (IoT) is one of the hottest topics in the IT world right now. The term 'Internet of Things' has piqued interest due to its depiction of a global network of connected physical things that enables anytime, everywhere networking for anything.

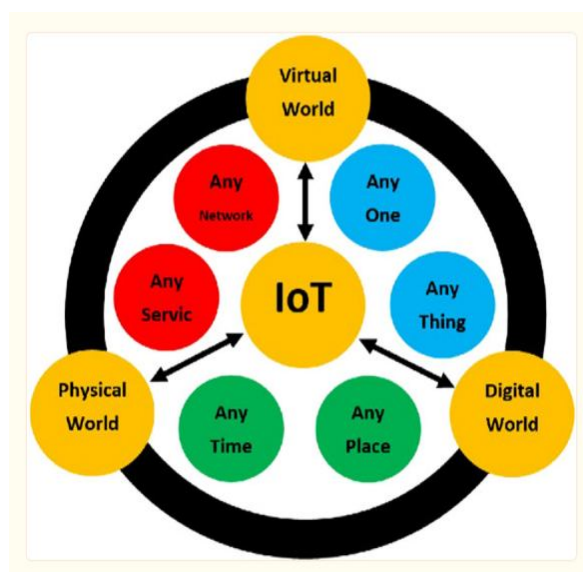


Fig 1. Internet of Things

This is a network that allows humans, things, and things to communicate using a unique identifier for each object. "Online schooling is not a new concept, but it has grown in popularity in the aftermath of the pandemic. The epidemic did not completely cease schooling, but it did require us to change our approach." "COVID-19" has questioned the long-term viability of systems and frameworks, particularly in informal educational environments where personal intercommunication and physical structures are prioritized. Given that large-scale disruptions are more likely to develop over the next decade due to pressures such as climate change, the pandemic has reduced the need for an educational approach to inventing stronger capacities for crisis response, including and beyond significant public health disasters. Students, parents and caregivers, educators, and decision-makers face both chronic and emergent ethical problems with heightened importance during COVID-19, as education and learning increasingly rely on digital platforms and resources. How can we seize the benefits while minimising the risks that come with mass adoption of digital technologies? What impact do these concerns have on diverse demographics and environments, what are the new challenges, gaps, and disparities in access, especially for marginalised or special needs communities? And, in COVID-disrupted places, how may current and persistent problems cause harm.

II. KEY THEMES

1. Disparities in access to Internet connectivity and digital devices include but extent beyond the rural-urban divide.

According to the LIRNEasia research, 64 percent of all houses with school-aged children had Internet connection, while the other 36 percent did not. The study also included a 7,000-home investigation across India, which included 350 villages and wards. Children in households with access to the internet were more likely to receive some form of remote learning, whereas just 8% of children in households without access to the internet claimed they received any form of learning. At the same time, a subsequent nationwide survey done by LIRNEasia revealed that Web usage had more than doubled in the previous four years, with Covid-related outages contributing to the increased demand for connectivity. In late 2017, 19% of the 15-65 age group claimed to have used the Internet, whereas 49 percent of the 15-65 age group claimed to have done so in late 2017. This translates to 61 percent of families using the Internet in 2021, up from 21% in 2017. In 2020 and 2021, it appeared that over 130 million clients went online. Of the almost 80 million people who started using the Internet in 2020, 43 percent, or more than 34 million, stated they started doing so after the Covid issue.

2. The widespread intensifies existing disparities but may offer assistance to make more obvious possible pathways to relieve inequities.

It is vital to assist in bridging the advanced divide that COVID-19 has created, while also recognising the pandemic's openings in order to alleviate imbalances. Participants talked on how the shift to online education has worsened educational disparities, which could have long-term consequences, especially for underrepresented groups. How can we think about learning and educational material from the bottom up (for example, in the context of informal learning spaces) to better level the playing field with such a large adolescent population? And how can we build policies that assist the development of youth skills while still being inclusive?

3. Human dignity preservation is vital in the educational system especially when viewed through the lens of certain ethical philosophies but it may be challenged in digitally mediated situations.

One question that came up during a discussion about the relevance of ethics in education was how do we conceive of ethics in education in a way that supports human dignity, especially for those who are marginalised? They advised looking into ethical frameworks from the Global South, such as Sub-Saharan Africa's Ubuntu concept, to preserve human dignity. This notion emphasises community belonging and the idea that for individuals to grow and be recognised in society, the community must be involved. Students particularly those from underrepresented communities may be more vulnerable to cyberbullying, surveillance, and opaque decision-making mechanisms as a result of more time spent online under COVID-19, constituting a danger to human dignity.

4. Inadequate or selectively represented data perpetuates inequality invisibly.

Covid-19 has demonstrated how underrepresented populations are usually left out of national statistics. For example, does not collect ethnicity or race information, indicating a lack of diversity and racial inequity in the country, which could hinder the development of equitable educational policies and programmes. To address inclusive development planning, we need a data lens that captures the reality on the ground. Digital inclusion will only happen when legislators establish policies that consider the entire community. To help enhance and develop educational programmes and policies, more data transparency and sharing on a global scale is also essential.

5. There are several privacy concerns, particularly as educational places and services undergo digital transition.

The collection and probable use of students' personal data, for example, presents security and privacy concerns in a virtual learning environment. Platforms that deliver online education typically collect enormous quantities of data from students. Currently, there is insufficient transparency about what data is collected, where it is stored, and how it might be used. The privacy risks may be magnified in specific geographical conditions (e.g., regions with more restrictive government policies). Academic institutions play a critical role in ensuring the privacy of students. Aside from top-down legislation, several participants stated that considering how varied stakeholders could collaborate to develop programmes and resources to solve online privacy issues could be beneficial (e.g., through the development of educational content, social contracts, etc.). Collaboration like this is especially important in areas where more awareness about these issues is needed. "When it comes to ethics, each stakeholder group has different wants and needs, which can often conflict.

[illegible]

The diagram illustrates eight challenges of data security, arranged in two rows and connected by a line. Each challenge is represented by an icon, a number, and a brief description.

- #1: Embedding data privacy** - Icon: A green shield with a white checkmark on a blue base.
- #2: Proliferating devices** - Icon: A laptop with a person icon on the screen and a document on the keyboard.
- #3: Increasing maintenance costs** - Icon: A green bar chart with a yellow coin on top.
- #4: Access control is difficult in many industries** - Icon: A red cube with a blue padlock on the front face.
- #5: Getting visibility into all your data** - Icon: A blue magnifying glass over a bar chart.
- #6: A bad data culture** - Icon: A green shield with a white checkmark on a yellow base.
- #7: The ever-increasing scale of data** - Icon: A blue globe with a green bar chart on top.
- #8: A long list of regulations and documentation to follow** - Icon: A blue book with a white checkmark on the cover.

Page-718

Data privacy: This refers to our legal obligation to protect the privacy of our personal information and to those who responsibly manage personal data. In other words, the law defines how you should obtain, keep, distribute, and allow access to personal data.

Cyber security: We need encryption and firewalls to protect data from compromise, corruption, and loss. In addition to cyber security, it includes backup and business continuity planning.

Compliance: Whether they are tied to technology or organisational policies and procedures, data privacy requirements must be obeyed by satisfying particular standards.

3.1 Data Collection Requires Digital Ethics.



Fig 4.General Data Protection Regulation

The General Data Protection Regulation (GDPR) allows schools, colleges, and universities to collect and use personal data if they claim to be working on a public-interest project. However, they must seek clear authorization before using personal data for any purpose other than their customary responsibilities as learning providers. It must come from their parents in the event of minors. All educational providers must collect data in a transparent manner in order to be compliant. E-learning providers, on the other hand, must pay more attention to signup forms, online checkouts, and the wording of their privacy policies. Privacy notices should be widely available, well-presented, and written in a manner that students of varied ages and reading levels can comprehend. They must discuss and outline what you do with student data:

3.2 Data Protection



Fig 5. Data Protection Policy

To meet the requirements of any data protection regulation, institutions will need to build suitable technical and organisational processes. In order to successfully secure people's privacy. Malware can be spread unintentionally by students via email, flash drives, and social media (particularly in an educational setting). Not only are that, but busy professors and lecturers with a mountain of emails and term-time job limitations obvious candidates for malware attachments and dangerous website URLs. This is why personnel must be trained in security awareness. In addition, we must ensure the following. The most recent software updates and fixes are installed on all software and workstations. Make it a habit to do so. There is a stringent password policy in place, and access capabilities are limited to only those users who need them to do their tasks. Only approved entities have access to classroom hardware. Examine the same. Defining protective data privacy rules to restrict where that data is collected, processed, and secured becomes difficult with so many requirements to meet. Regardless, it is crucial in every industry, including education.

This is when privacy laws come into play, allowing citizens to request that their personal information be erased. A high level of oversight is required in the education industry. Using technologies that provide a full picture of all of our data, we can achieve the same results. It will allow us to accurately deliver all stored information on an individual, as well as swiftly and efficiently respond to enquiries.

IV. CONCLUSION

Without a doubt, technological advancements are supporting us in crafting a bright future by allowing all major industries to change their identities and better serve the general population. However, there is a considerable risk to consumers' data and privacy as a result of all of this. This vulnerability is amplified in the education sector, which must protect a vast amount of user data. Knowing all of these digital ethics, as well as our privacy rights, will help us become better educated users and make better decisions.

REFERENCES

1. "A conceptual framework for digital civics pedagogy informed by the philosophy of information", Clements, E. (2019), Journal of Documentation, 76(2), 571-585. <https://doi.org/10.1108/JD-07-2019-0139>.
2. "Cascading morality after Dewey: A proposal for a pluralist meta-ethics with a subsidiarity hierarchy-Contemporary Pragmatism", Coeckelbergh, M. (2021). 18(1), 18. <https://doi.org/10.1163/18758185-bja10002>
3. "Teaching data ethics: We're going to ethics the heck out of this", Henderson, T. (2019), Proceedings of the 3rd Conference on Computing Education Practice. <https://doi.org/10.1145/3294016.3294017>
4. "Automating Inequality. How High-Tech Tools Profile, Police and Punish the Poor" Eubanks. V. (2018) St. Martin's Press.
5. "Embedded Ethics: Integrating ethics across CS education", Grosz, B. J. et al. (2019) Communications of the ACM, 62(8), 61. <https://doi.org/10.1145/3330794>.