



DigitalRightsFoundation



# VIRTUAL LEARNING AND PRIVACY AMID COVID-19

---

A RESEARCH BY DIGITAL RIGHTS FOUNDATION



## About

Digital Rights Foundation (DRF) is a Digital Rights Foundation (DRF) is a feminist, not-for-profit organisation based in Pakistan working on digital freedoms since 2013. DRF envisions a place where all people, especially women and gender minorities, can exercise their right of expression without being threatened.

DRF believes that a free internet with access to information and impeccable privacy policies can create safe online spaces for not only women but the world at large.

### **Contact information:**

[info@digitalrightsfoundation.pk](mailto:info@digitalrightsfoundation.pk)  
[www.digitalrightsfoundation.pk](http://www.digitalrightsfoundation.pk)

## **Acknowledgements**

This report would not have been possible without the hard work of our research team comprising of ShehrBano Hassan, Zainab Durrani and Zaman Karamat; and the revision and editing by the Head of Research and Policy, Shmyla Khan, the design work by Ahsan Zahid and Talha Umar and the support of Privacy International.

We are also grateful to all the individuals who agreed to participate in our research and provided the valuable data that make up the findings and analysis of this report.

# Table of Content

Executive Summary	01
a. Main objectives	
b. Key outcomes	
Introduction	03
Methodology	05
Limitations	06
Literature Review	07
a. Privacy risks and harms amid COVID-19	
b. The rise of e-learning around the world	
c. Student Privacy amid COVID 19	
d. Pakistan: e-learning platforms and the HEC	
e. PECA and data privacy loopholes	
Findings and Discussion	15
a. Participant demographics	
b. The state of privacy	
c. Data collection, data access and storage	
d. Privacy harms and risks	
Recommendations	24
a. For education departments and administrators	
b. For the state	
c. For civil society actors	
d. Direct recommendations from consultations	
Conclusion	28
References	29

# Executive Summary

This research was motivated by the desire to understand the ways in which student and teacher privacy was impacted by the switch to virtual learning, as a result of the COVID-19 pandemic. Though digitalisation was already embedded within the daily lives of human beings long ago, the COVID-19 pandemic brought about an unprecedented escalation of reliance on digital forms of communication, including social media and online platforms. With physical connections eroding, this was undoubtedly a welcome advancement. However, the dangers of such technologies and their usage has not been investigated in their entirety, particularly in countries in the Global South.

Coupled with the weak legislative and institutional infrastructure of countries like Pakistan, it becomes particularly imperative to investigate whether appropriate checks and balances exist to ensure and protect the privacy of individuals. Pakistan also currently does not have a specific data protection law nor does it have any legislation allowing individuals the right to request data about themselves. The main governing legislation around crimes in the digital sphere is PECA (Prevention of Electronic Crimes Act 2016), which has come under severe criticism for its harsh penalties and potential for abuse and misuse. In fact, matters of data privacy and protection are relatively new areas of concern for the Pakistani government and society in general.

In light of this, the aim of this study was to conduct comprehensive research to understand the ways in which the shift to online/remote learning has impacted students' privacy and whether educational institutions have adequate policies in place to deal with these new challenges.

# Main objectives

- Map and understand the experiences of students with regards to privacy perceptions, risks and harms associated with using online learning platforms
- Investigate the privacy practices between students, teachers and educational institutions
- Contribute to literature on privacy experiences and practices during COVID-19
- Use the research as a baseline study to design workshops and training sessions around ensuring privacy protections in specific educational institutions

# Key outcomes

- There is a significant gap in understanding and practices around privacy between government, educational institutions and individuals within the education sector
- This is particularly relevant in areas of consent (with regards to recording lectures and other multimedia content) as well as data storage, collection, and access practices
- This is largely due to a lack of awareness and understanding around the importance of privacy across the country
- Students and teachers, particularly female ones, are most adversely impacted by the lack of privacy regulation

# Introduction

The year 2020 was defined by two things: the onset and spread of the COVID-19 pandemic, and the increased digitalisation that it brought about. This digitalisation has had a major impact on many spheres of life around the world, one of which has been the expansion of the e-learning education model, particularly through the use of communication platforms. This assertion is supported by the World Economic Forum, which notes that the pandemic has resulted in a mass switch to e-learning and consequently, changed the way education is practiced around the world forever.<sup>1</sup> UNESCO reports that close to half the world's students are still affected by partial or full school closures.<sup>2</sup> Simultaneously, there has been a significant surge in language apps, virtual tutoring and e-learning software, as well as video conferencing tools.<sup>3</sup> Though a welcome development and advance in technology, certain areas of concern have undoubtedly been overlooked. Where these concerns have been observed and addressed, the data relates mostly to users in the Global North. For example, the decision to shift to online learning ignited a fresh discussion around student and teacher privacy concerns.<sup>4</sup>

Whereas in the offline world, issues of protecting student data and secure storage of students' personal details have been a persistent concern, the shift to e-learning has brought about additional issues, such as unauthorised use of e-learning platforms, lack of privacy protocols within institutions and absence of vetting around virtual learning softwares.<sup>5</sup> Video conferencing platforms such as Zoom and Skype have faced significant privacy breaches<sup>6</sup> since the onset of the pandemic. Moreover, these incidents haven't just affected these popular digital platforms but have directly affected education institutions. Several high-profile universities and educational institutions, including Stanford Medical School and the University of California, have been involved in breaches that exposed their students' sensitive information, including names, addresses, and Social Security numbers.<sup>7</sup> Considering the fragile nature of these platforms, student data is understandably at risk of breaches and

---

<sup>1</sup> <https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/>

<sup>2</sup> <https://en.unesco.org/covid19/educationresponse#schoolclosures>

<sup>3</sup> <https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/>

<sup>4</sup> <https://iapp.org/news/a/shift-to-online-learning-ignites-student-privacy-concerns/>

<sup>5</sup> <https://iapp.org/news/a/shift-to-online-learning-ignites-student-privacy-concerns/>

<sup>6</sup> <https://www.tomsguide.com/uk/news/zoom-security-privacy-woes>

<sup>7</sup> <https://thehill.com/opinion/technology/550959-massive-school-data-breach-shows-we-need-better-privacy-policies>

leaks. Furthermore, due to weak institutional checks<sup>8</sup> in Pakistan, it is particularly vital to identify the gaps in directives between government, educational institutions and students in order to understand how student data may be unknowingly at risk. Pakistani society is no stranger to privacy breaches and violations.<sup>9</sup> Even prior to the COVID-19 pandemic, Pakistan has had to reckon with the expansion of its public space into the unregulated free-for-all domain of the online world. As such, privacy breaches involving young people, particularly women, are not uncommon. In fact, Digital Rights Foundation's own cyber harassment hotline observed an increase in cases of blackmailing using individuals' sensitive content and information during COVID-19.<sup>10</sup> With an increased number of individuals relying on online platforms to stay connected, the risks and harms associated with online spaces in Pakistan also increased simultaneously, including the risks of privacy violations and misuse of data.

In light of these observations, this study seeks to understand the ways in which the shift to virtual learning has impacted the way privacy is practiced and understood in educational institutions in Pakistan, particularly through the investigation of the use of communication platforms. Additionally, it highlights whether these bodies have adequate policies in place to deal with these new and emerging challenges.

---

<sup>8</sup> <https://www.wilsoncenter.org/sites/default/files/media/documents/publication/2018-06-pakistansinstitutions.pdf>

<sup>9</sup> <https://www.thenews.com.pk/tns/detail/586618-cyber-insecurity>

<sup>10</sup> <https://digitalrightsfoundation.pk/wp-content/uploads/2021/03/Annual-Report-2020.pdf>

# Methodology

Both quantitative and qualitative data was gathered for this research, through surveys and interviews with students, teachers and administrators from various educational institutions. Both public and private schools and universities were considered in the study. The first stage of data collection was an online survey, hosted on Google Forms, disseminated across social media and specific stakeholder networks. A total of 131 participants were surveyed. Through this, we gathered our initial set of participants including students, parents of students documenting their children's experiences, teachers and school administrators. This questionnaire provided the basis for examining students, teachers and school administrator experiences of virtual learning and privacy during COVID-19. It also allowed us to map themes to explore in follow up interviews; our second stage of data collection. We also directly reached out to specific public and private schools to interview teachers and administrators. We conducted a total of 11 interviews with students, teachers and administrators from across Pakistan. This data was essential to identify the gaps between government policy, school policy and individual experiences of students and teachers as they experience virtual learning.

Additionally focus group discussions were conducted with two groups of 5 educators each as well as a separate consultation session with 4 members of a private school based in Pakistan to glean their experience of participating in virtual learning and to ask them for their recommendations on what a model privacy policy document would look like, from their perspective.

Finally, data from the questionnaire, consultations and interviews was compiled and analysed. The insights from these findings are provided in this report and supported by a literature review.



# Limitations

It must be noted that this study does not claim to capture the experiences of all students, teachers or administrators engaged in virtual remote learning in Pakistan. Indeed, there are experiences that are not represented within this study purely due to the nature of the methodology, particularly with regards to students who were unable to engage in remote learning due to lack of resources, such as internet connectivity. Moreover, private school students and teachers were also disproportionately represented due to the process of dissemination as a result of the ongoing COVID-19 pandemic. Therefore, to make generalized inferences based on this dataset would be an error. Furthermore, data-gathering was hindered due to various issues such as limited availability of participants and internet connectivity problems. With a greater data set and increased respondents, the findings may be substantiated and strengthened further.

# Literature review

## 1. Privacy risks and harms amid COVID-19

The pandemic has had many effects; one of which is emboldening the fragile and conditional nature of privacy as a key concern in the global arena. Since the start of the COVID-19 pandemic, organisations have observed repeated patterns of data breaches, tracking and surveillance by governments and data violations as signs of a sidelining of individual and collective privacy amid global crisis.<sup>11</sup> Privacy, an inalienable right of the individual, enshrined in constitutions around the world and in human rights conventions,<sup>12</sup> now seems to be conditional on the absence of global emergencies. This has led Alessandra Pierucci, Chair of the Council of Europe's data protection committee to state that there should not have to be a choice made between saving lives and protecting our privacy - the issue is one of reconciling fundamental rights.<sup>13</sup> Corroborating this, Zwitter and Gstrein found that legal frameworks including redress mechanisms are currently not capable of effectively ensuring data protection, since they focus too much on the individual.<sup>14</sup> Indeed, violations involving social media accounts and Zoom or Skype accounts have seen a sharp increase since the pandemic.<sup>15</sup> For example, early investigations by the FTC found that Zoom's end-to-end encryption was not guaranteed.<sup>16</sup> Though this issue was later resolved after Zoom came under fire, other privacy issues have yet to be addressed by the popular app. For example, a common prank involving individuals - often teenagers - attending private meetings on Zoom and sharing shocking explicit content has come to be referred to as "Zoombombing".<sup>17</sup>

Furthermore, perceptions and legal understandings of privacy fail to account for violations of collective privacy, through data gathering, access and storage activities or collection by institutions. This includes governments monitoring, collecting

---

<sup>11</sup> <https://privacyinternational.org/examples/tracking-global-response-covid-19>

<sup>12</sup> <http://gilc.org/privacy/survey/intro.html#:~:text=Privacy%20is%20a%20fundamental%20human,association%20and%20freedom%20of%20speech.>

<sup>13</sup> <https://www.coe.int/en/web/portal/covid-19-health-and-privacy>

<sup>14</sup> <https://jhumanitarianaction.springeropen.com/articles/10.1186/s41018-020-00072-6>

<sup>15</sup> <https://arxiv.org/pdf/2103.01779.pdf>

<sup>16</sup> <https://arstechnica.com/tech-policy/2020/11/zoom-lied-to-users-about-end-to-end-encryption-for-years-ftc-says/>

<sup>17</sup> <https://www.forbes.com/sites/kateoflahertyuk/2020/03/27/beware-zoom-users-heres-how-people-can-zoom-bomb-your-chat/>

and storing health data through contact tracing and self-reporting apps.<sup>18</sup> For example, several countries, such as China, South Korea and Pakistan, have developed contact tracing apps that are based on the analysis of location data collected through phone networks, WiFi connections, and satellite-based radio navigation systems.<sup>19</sup> This means that data protection frameworks remain inadequate in addressing collective privacy violations due to their emphasis on and roots in individual understandings of privacy.

## 2. The rise of e-learning around the world

UNESCO reports that over 1.2 billion children in over 186 countries have been affected by school closures in 2020.<sup>20</sup> The closure of schools allowed for a vacuum to be created, which was filled almost immediately by e-learning platforms and forums.<sup>21</sup> Universities, schools and colleges around the world had to switch their operations entirely online with the help of educational technology. Global interest and adoption of EdTech was high, with global investments reaching 18.66 billion dollars in 2019, the industry has seen an unprecedented surge since COVID-19.<sup>22</sup> Similarly, there has been a significant rise in other forms of virtual learning, including language apps, virtual tutoring, and online learning software. For example, enrollments at Coursera, an online platform that offers free online courses, were up 640% in April 2020 compared to April 2019 and Udemy, a similar platform, experienced a 400% increase between February and March 2020.<sup>23</sup> Major investments and development into the EdTech industry have allowed distanced virtual learning to become easier.<sup>24</sup> For instance, the ability to use a computer connected to a network offers the possibility to learn from anywhere around the world, at any time.<sup>25</sup>

In these environments, students can be anywhere to learn and interact with instructors and other students.<sup>26</sup> In such a learning environment, the more traditional live

---

<sup>18</sup> <https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/privacy-security-and-public-health-in-a-pandemic-year>

<sup>19</sup> <https://jhumanitarianaction.springeropen.com/articles/10.1186/s41018-020-00072-6>

<sup>20</sup> <https://en.unesco.org/covid19/educationresponse#schoolclosures>

<sup>21</sup> <https://www.tandfonline.com/doi/full/10.1080/10494820.2020.1813180>

<sup>22</sup> <https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/>

<sup>23</sup> <https://www.orange-business.com/en/blogs/top-class-pandemic-powered-rise-distance-learning>

<sup>24</sup> <https://journals.sagepub.com/doi/full/10.1177/0047239520934018#>

<sup>25</sup> Cojocariu, V.-M., Lazar, I., Nedeff, V., Lazar, G. (2014). SWOT analysis of e-learning educational services from the perspective of their beneficiaries. *Procedia-Social and Behavioral Sciences*, 116, 1999–2003.

<sup>26</sup> Singh, V., Thurman, A. (2019). How many ways can we define online learning? A systematic literature review of definitions of online learning (1988-2018). *American Journal of Distance Education*, 33(4), 289–306.

in-person lectures or classes are replaced by content made available on different learning platforms and forums. In particular, learners in the most marginalized groups, who don't have access to digital learning resources or lack the resilience and engagement to learn on their own, are at risk of falling behind.<sup>27</sup> Moreover, weak course content that doesn't engage students where there is a vacuum of physical interaction and dynamics is also a major issue.<sup>28</sup> Song et al found that students register a lack of collectivism, technical issues and difficulties grasping instructions in online learning.<sup>29</sup> A similar study found that students were unable to balance their work, family, and social lives with their study lives in an online learning environment.<sup>30</sup> It is evident from this that while the development of the EdTech industry has been welcomed during a crisis, it does not come without several drawbacks; one of which is concerns over student privacy, data collection and safety.

### 3. Student Privacy amid COVID 19

The education sector was reportedly responsible for 884 million leaked records across the globe in 2020, making it the third most affected by data breaches.<sup>31</sup> School administrators have been faced with tough questions and decisions in the wake of the COVID-19 pandemic and the resulting school closures. One of the many concerns has been the protection of student privacy and data. According to the OECD, teachers have had to adapt to new “modes of delivery of teaching, for which they may not have been trained”.<sup>32</sup> Administrators in both schools and universities have had to grapple with striking a balance between maintaining the privacy of students and ensuring that the quality of education does not deteriorate. Privacy concerns with regards to remote learning include images and videos being captured and recorded via video-conferencing tools. These efforts involve collecting sensitive information on students and employees; data that schools are required to safeguard.

---

<sup>27</sup> <https://www.irissexaminer.com/news/arid-40342238.html>

<sup>28</sup> <https://docs.edtechhub.org/lib/9TKV7H6E/download/3LMTWFGC/Baloch%20et%20al.%20-%202020%20-%20Pakistan%20Topic%20Brief%20Providing%20Distance%20Learning%20.pdf>

<sup>29</sup> Song, L., Singleton, E. S., Hill, J. R., Koh, M. H. (2004). Improving online learning: Student perceptions of useful and challenging characteristics. *The Internet and Higher Education*, 7(1), 59–70.

<sup>30</sup> Parkes, M., Stein, S., Reading, C. (2014). Student preparedness for university e-learning environments. *The Internet and Higher Education*, 25, 1–10. <https://doi.org/10.1016/j.iheduc.2014.10.002>

<sup>31</sup> <https://techhq.com/2021/07/education-sector-hardest-hit-by-ransomware-in-2020/>

<sup>32</sup> <https://www.oecd.org/education/the-impact-of-covid-19-on-education-insights-education-at-a-glance-2020.pdf>

Indeed, cases of privacy and security violations are not a new phenomenon. According to a report by Ellucian, 17% of all data breaches in the past decade occurred in higher education – the second highest of any industry besides healthcare.<sup>33</sup> Cybersecurity firm Bluevoyant found that higher education institutions continue to have “problematic password policies, lack multifactor authentication (MFA), and a plethora of open ports — despite suffering dozens of ransomware attacks and targeting by attackers focused on stealing student information”.<sup>34</sup> Similarly, according to Common Sense, an American non-profit that evaluates EdTech tools, 80% of the applications and services they reviewed in 2019 did not meet their minimum level of responsible safeguards.<sup>35</sup> This vulnerability directly relates to security breaches in schools and universities. Universally, the sharp rise in breaches have shed a much-needed light on the vulnerability of student data and the lack of protections in place to secure them from such violations. For example, in April 2021, over 100 universities were hit with a data breach through a third-party file-transfer application that accessed information including names, addresses, telephone numbers, birth dates, social security numbers and bank account information for “employees and their dependents and beneficiaries, retirees and their beneficiaries, students and their families”.<sup>36</sup> This violation came only a few weeks after a major data breach in the American University’s online portal, exposing over 6000 students’ confidential information.<sup>37</sup> Beyond universities, e-learning platforms have also suffered major data breaches. Indian e-learning platform Edureka, operating in the US, was found to be using unsecure servers, publicly making available more than 25 gigabytes of personal information belonging to around 2 million Edureka users.<sup>38</sup>

These concerns over privacy are not limited to school administrators and human rights organisations. Research shows that generally, the data of minors is universally acknowledged to enjoy and require greater protections.<sup>39</sup> However, even older students’ lack of understanding about how their institution uses personal data undermines

---

<sup>33</sup> <https://www.virtu.com/blog/university-data-protection-2/>

<sup>34</sup> <https://www.darkreading.com/attacks-breaches/universities-face-double-threat-of-ransomware-data-breaches>

<sup>35</sup> <https://privacy.commonsense.org/resource/2019-state-of-edtech-privacy-report>

<sup>36</sup> <https://thehill.com/opinion/technology/550959-massive-school-data-breach-shows-we-need-better-privacy-policies>

<sup>37</sup> <https://www.theeagleonline.com/article/2021/04/au-unintentionally-exposed-thousands-of-students-data-in-violation-of-federal-law>

<sup>38</sup> <https://www.safetydetectives.com/blog/edureka-leak-report/>

<sup>39</sup> <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf>

both their trust in that use and their confidence in how their institution protects personal data. Moreover, students' lack of confidence in their institution's ability to safeguard their personal data is rooted in their belief that their institution is vulnerable to attack and lacking in transparency.<sup>40</sup> It should be noted that such violations and concerns are not limited to the Global North. However, due to the patterns of reporting and under-developed standards to regulate privacy breaches, the Global South is still underrepresented in the discourse on data privacy in e-learning.

#### **4. Pakistan: e-learning platforms and the HEC**

This section addresses the use of e-learning within higher education institutions across Pakistan. E-learning or distance learning also made a place for itself in Pakistan, in private and public institutions, such as Virtual University, COMSATS University<sup>41</sup> and Allama Iqbal Open University (established in 1974).<sup>42</sup> The cases mentioned above have used digital technologies to provide academic instruction to students from all over the country and the world; Virtual University is entirely digital and broadcasts its lessons over cable television, YouTube and DailyMotion.<sup>43</sup> COMSATS University established a dedicated virtual campus that helped educate students from rural Pakistan who could not attend university because of “inflexible timings, cost, or cultural barriers.”<sup>44</sup> Furthermore, the Punjab Government launched an e-learning campaign called “ELearn.Punjab” in 2014 — a first-of-its-kind initiative in Pakistan that allowed students to access academic resources digitally.<sup>45</sup>

The Higher Education Commission (HEC) of Pakistan has been working on multiple projects to integrate e-learning technologies into the education system over the past few decades. The “Pakistan Education and Research Network” (PERN), “Pakistan Research Repository” (PRR), and projects featuring tools such as online lecturing and video conferencing have been in the works since 2006.<sup>46</sup> However, the pandemic demanded an increase in capacity for e-learning since most, if not all, educational institutions experienced some type of closure. Continued closure without some

---

<sup>40</sup> <https://www.virtu.com/blog/university-data-protection-2/>

<sup>41</sup> <https://vcomsats.edu.pk/about/how-it-works>

<sup>42</sup> [www.aiou.edu.pk](http://www.aiou.edu.pk). Retrieved 4 August 2019.

<sup>43</sup> *ibid*

<sup>44</sup> <https://vcomsats.edu.pk/about/introduction>

<sup>45</sup> [https://www.academia.edu/39702296/Emerging\\_Trends\\_of\\_E\\_Learning\\_in\\_Pakistan\\_Past\\_Present\\_and\\_Future](https://www.academia.edu/39702296/Emerging_Trends_of_E_Learning_in_Pakistan_Past_Present_and_Future)

<sup>46</sup> <https://elearnmag.acm.org/featured.cfm?aid=2668882>

form of synchronous or asynchronous learning could be financially catastrophic for institutions, as the HEC (2020) highlighted in their guidelines:

“The loss of a full semester will also be a loss for the universities. The lost semester will have to be substituted for later, without receipt of additional tuition fees, thus imposing an unaffordable financial burden on universities, especially problematic for public sector universities, given the current financial straits created by past budget cuts.”<sup>47</sup>

The mass implementation of e-learning or remote learning appeared to be the solution to this predicament. As found by a survey conducted by the HEC, very few universities had operational Learning Management Systems and video conferencing capabilities,<sup>48</sup> prior to the Covid-19 pandemic; approximately seventy out of one hundred and ten public sector universities did not have basic Learning Management Systems and forty did not have video conferencing capabilities. In order to “ensure that teaching continues wherever possible” and that “disruption on the students’ learning is minimised”, the HEC formulated a set of guidelines, requirements and policies, and created a Technology Support Committee to guide educational institutions on how to operationalise remote learning.<sup>49</sup> These guidelines outlined the essential features required for remote instruction and made recommendations on what software to use, such as Microsoft Teams, Zoom, Moodle, Adobe Connect and more.<sup>50</sup>

The HEC provided universities on the Pakistan Education and Research Network (PERN) with free Microsoft 365 subscriptions which include the use of Microsoft Teams — a video conferencing platform — while giving other institutions six months of coverage.<sup>51</sup> An adoption timeline was shared with universities in March 2020, and since then, according to the HEC, universities have begun transitioning or have transitioned to remote learning, even if it is at a “basic level”.<sup>52</sup> The rapid virtualisation of the education sector faced many challenges; teachers lacked

---

<sup>47</sup> <https://hec.gov.pk/english/HECAnnouncements/Documents/nCoVirus/Government-Directive.pdf>

<sup>48</sup> <https://hec.gov.pk/english/HECAnnouncements/Documents/nCoVirus/Approved-Working-Paper.pdf>

<sup>49</sup> Ibid

<sup>50</sup> Ibid

<sup>51</sup> Ibid

<sup>52</sup> <https://hec.gov.pk/english/HECAnnouncements/Documents/nCoVirus/Covid-19-Policy-Guidance-No.5-Online%20Readiness.pdf>

training, students often encountered connectivity and technology challenges, and the quality of education was called into question.<sup>53</sup> Though the government and HEC have attempted to address these issues through guidelines and training, legislative and institutional drawbacks have hindered the protection of student privacy and data protection in an efficient and comprehensive manner.<sup>54</sup>

## 5. PECA and data privacy loopholes

As per Bolo Bhi's observations,<sup>55</sup> a digital rights organization in Pakistan, the Prevention of Electronic Crimes Act 2016<sup>56</sup> came in as a continuation of the efforts to align legislative actions with the 12-Point National Action Plan (NAP)<sup>57</sup> developed in the aftermath of the APS School Peshawar attack of 2014<sup>58</sup> in which 150 lives were lost. The cybercrime law reflects this through several of its sections where individual interest is seemingly put aside to focus on public interest, including section 32 which necessitates the retention of traffic data by service providers for a minimum period of one year unless directed to do so for longer by the Pakistan Telecommunication Authority which is the relevant law enforcement agency under this Act.

Some of the concerns highlighted in the 2015 Legal Analysis<sup>59</sup> released by DRF in collaboration with Privacy International on the then draft Prevention of Electronic Crime Bill are still relevant when penning this report today: "A clear and accessible legal regime compliant with international law should govern any data copied by state authorities". This concern is unaddressed to date as Pakistan still does not have a legal regime that oversees and regulates the collection and processing of data of the country's citizens, particularly in the absence of data protection legislation.

Section 31 of PECA empowers the FIA to acquire data provided that such data is required for criminal investigation and there is a threat that it may be "modified, lost, destroyed or rendered inaccessible". FIA can also apply for search and seizure of data and disclosure of content data under section 33 and 34 of PECA. Under section 35, FIA can also acquire data in an unencrypted or decrypted format.

---

<sup>53</sup> <https://hec.gov.pk/english/HECAnnouncements/Documents/nCoVirus/Government-Directive.pdf>

<sup>54</sup> <https://www.wilsoncenter.org/sites/default/files/media/documents/publication/2018-06-pakistansinstitutions.pdf>

<sup>55</sup> <https://bolobhi.org/archive-prevention-electronic-crimes-bill-2015/>

<sup>56</sup> [https://na.gov.pk/uploads/documents/1470910659\\_707.pdf](https://na.gov.pk/uploads/documents/1470910659_707.pdf)

<sup>57</sup> <https://nacta.gov.pk/nap-2014/>

<sup>58</sup> <https://www.bbc.co.uk/news/world-asia-30491435>

<sup>59</sup> [https://digitalrightsfoundation.pk/wp-content/uploads/2015/04/Prevention-of-Electronic-Crimes-Bill-2015-Legal-Analysis\\_0.pdf](https://digitalrightsfoundation.pk/wp-content/uploads/2015/04/Prevention-of-Electronic-Crimes-Bill-2015-Legal-Analysis_0.pdf)



Moreover, section 32 of PECA requires a service provider to retain traffic data for a minimum of one year and this period can be increased by the PTA. Section 33 details the authority to confiscate any information system, data or device, Section 34 allows an authorised officer of the investigation to ask the court for a warrant for disclosure of content data and Section 39 also provides for real time collection and recording of information if it is required for a criminal investigation and after obtaining a court order in this respect. As per an analysis of PECA published in the LUMS Law Journal:<sup>60</sup>

“In pure constitutional terms, PECA violates Articles 4, 10-A, 14, and 19 of the Constitution of the Islamic Republic of Pakistan 1973. The aforementioned articles relate to certain universal fundamental rights which are the cornerstones of a democratic polity. Therefore, it is important that they should not be sidelined in the name of national security.”<sup>61</sup>

These elements should be specifically enumerated and governed by a clear and accessible legal regime that provides for redress for any violations of the right to privacy. Data should not be retained for longer than is necessary, given the purposes for which it was collected. Nor should it be used for purposes outside those specified in the law.

---

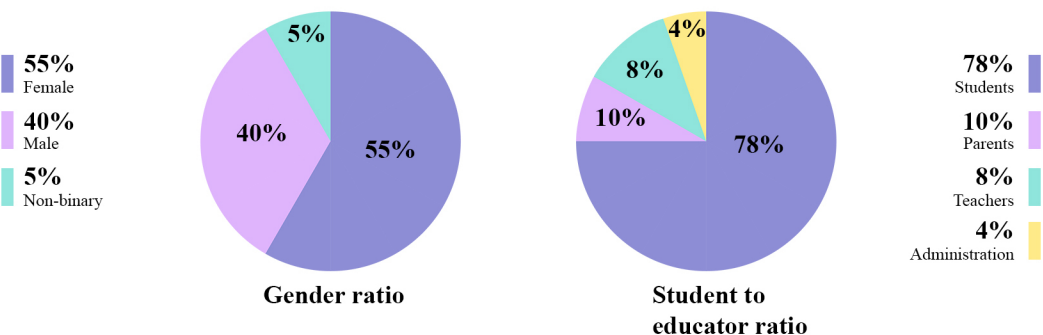
<sup>60</sup> <https://sahsol.lums.edu.pk/law-journal/prevention-electronic-crimes-act-2016-analysis>

<sup>61</sup> <https://sahsol.lums.edu.pk/law-journal/prevention-electronic-crimes-act-2016-analysis>.

# Findings and Discussion

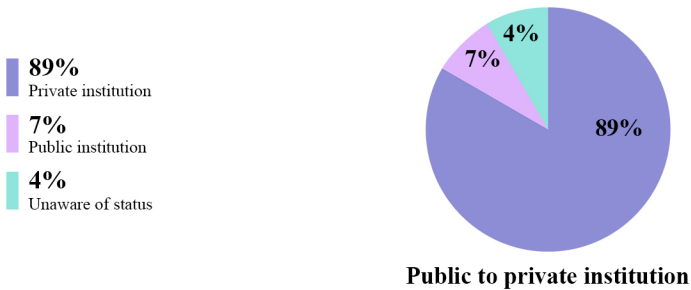
## 1. Participant demographics

Of the 131 participants surveyed and interviewed, 55% respondents self-identified as female, 40% male while 5 respondents listed themselves as either non-binary, genderfluid or preferred not to state their gender entirely. 78% identified themselves as registered students while 10% stated that they were parents or guardians of current students. Alternatively, 7.5% selected their occupation as teachers while only 4% stated that they were part of school administration bodies. Geographically, the participants were concentrated in the urban regions, specifically main cities such as Lahore, Islamabad and Karachi with 90, 19 and 13 respondents respectively. Beyond this, there was 1 participant each from Mithi, Bahawalpur, Hyderabad, Rawalpindi, Gujranwala, Multan and 2 from Peshawar.



Within the specific student and parent/guardian set, there were 106 student respondents and 13 responses from parents/guardians. 89% of the respondents specified that their children attended a private school while 7% listed their related school as public/government-run. 4% of respondents in this set were unaware of the status of their school as public or private. Students and parents were also asked to list the name of their school and grade if they felt comfortable. Most opted to state the school name and grade. Listed schools and grades ranged from Kindergarten and daycare centres to senior schools and universities.

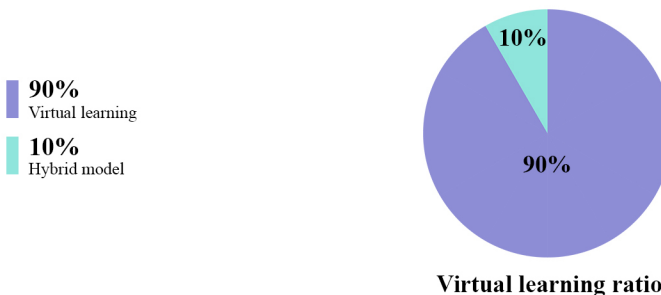
Of the 15 teachers and administrators, 13 were female while 2 were male. 10 listed themselves as teachers while 5 stated that they were administrators. 11 respondents in this group stated that they were associated with a private school while 4 were associated with public schools.

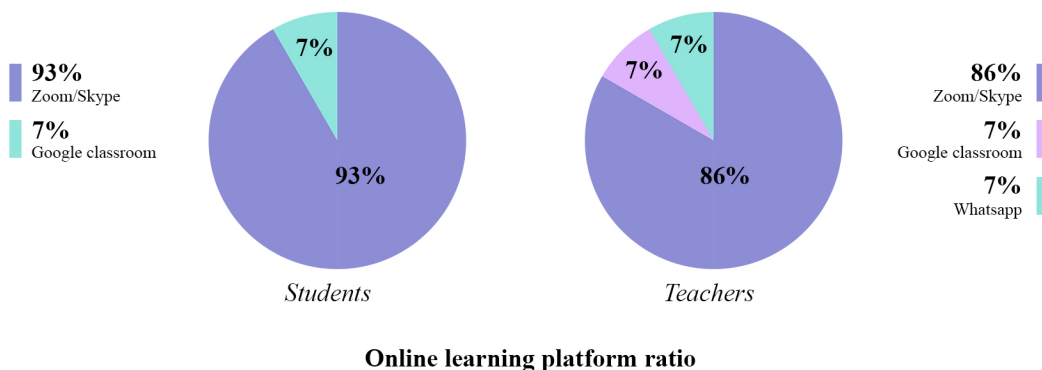


Of the 15 teachers and administrators, 13 were female while 2 were male. 10 listed themselves as teachers while 5 stated that they were administrators. 11 respondents in this group stated that they were associated with a private school while 4 were associated with public schools.

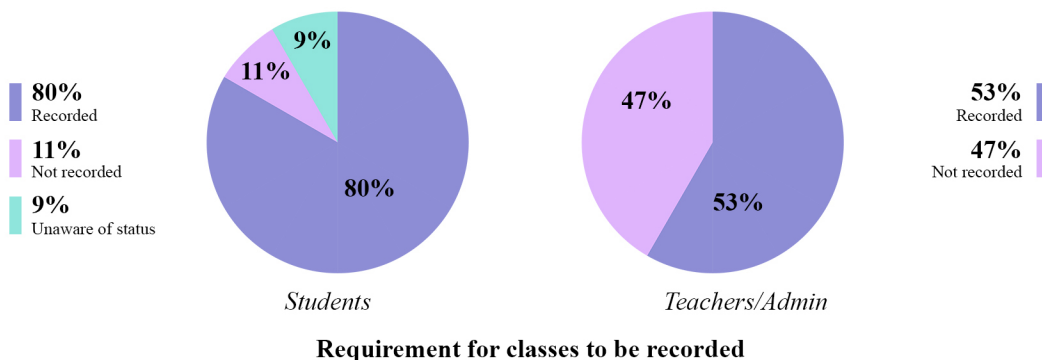
## 2. The state of privacy

Participants were asked a range of questions to explore the state of virtual learning and privacy in Pakistan as well as their specific institutions. This included understanding the extent to which virtual learning had been adopted, what platforms were used and what policies and measures were in place to regulate virtual learning. Out of the students and parents surveyed, 90% stated that virtual learning had been completely adopted by their associated institutions, while 10% stated that there was some partial adoption with a few hybrid models in place. All of the surveyed teachers and administrators stated that their schools had switched to virtual learning. The survey also asked respondents to confirm whether they were using services such as Zoom or Skype. 93% of students and parents stated they were using these services for online learning, while 7% stated they had switched to Google Classroom. Of the teachers and administrators, 87% used Zoom or Skype, 7% used Google Classroom, while another 7% used WhatsApp. Given the risks associated with the use of video conferencing platforms such as Zoom and Skype, particularly data breaches and cases of “zoombombing”, the increased use of these platforms in Pakistan could indicate an increased risk of privacy violations in schools if necessary protections aren’t adopted.





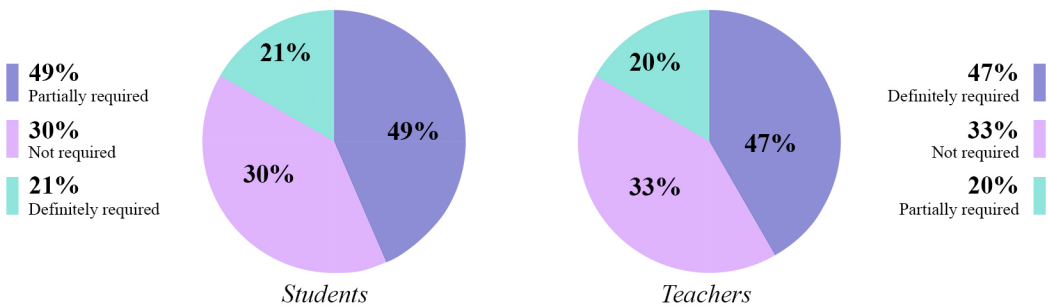
Delving deeper into institutional privacy practices, participants were asked about whether their institutions recorded online classes. 80% of students and parents stated their schools recorded online classes, while 11% stated that their schools did not record classes, while 9% of students / parents did not know whether their school recorded classes. 53% of teachers and administrators confirmed the recording of online classes while 47% said no recordings were made. The requirement to keep cameras on begs the question of where the recordings are stored once the class ends, how long the recordings are stored for and who has access to that data. In the interviews, students stated that they were not asked for consent before classes were recorded:



**“No, there was no consent. We were told this class was going to be recorded.” [S6]**

**“Most of the time they'd tell us that we'll record this lecture and we'll give it to you guys. No consent per say.” [S1]**

This was a particularly concerning issue because the survey found that most students were required by their schools to keep their cameras on during virtual classes. Of the students and parent respondents, 49% stated that they were required to partially keep their cameras on while 30% stated they were not required. A further 21% stated they were definitely required to keep cameras on. This means that 70% of participants were at one point during virtual learning required to have their cameras on. This corresponded with the responses from teachers and administrators, 47% of which stated that there was a definite requirement for students to keep their cameras on. 33% stated that students were not required while 20% stated that there was a partial requirement to keep cameras on.



**Requirement for cameras to be switched on**

A further set of questions were directed at exploring the privacy policies around virtual learning and data handling in general. These also included questions around the guidance and training offered at the state-level and school level. When asked about the existence of a privacy policy in their institutions, 60% of teachers and administrators stated that a privacy policy existed. However, 53% stated that this policy was not easily accessible (i.e. in a written form or on the institution's website). 20% of teachers and administrators did not know whether a privacy policy existed while 20% stated that no such policy existed in their school.

**“I’m not aware of any such rules. I wasn’t given any exposure to the privacy policy. My institution might have one but I am personally not aware of any such policies.” [T2]**

**“We do have policies regarding dress codes, subjects being offered and the scholarships policy. We do have those policies but we do not have any policy regarding children’s privacy and anything like that” [A1]**

**“I wouldn’t be surprised if my university does not have a privacy policy. In the induction process or since then, I have not come across a privacy policy.” [T2]**

In response to the question around training for virtual learning, 54.3% of students and parents stated that they were not given any training and information, while 37% stated they were given some information or training while 9% said they were not sure. 80% of teachers and administrators stated that they were also given some training and information before commencing virtual learning. During their interviews, participants were also asked whether they were given any guidance from the government. All respondents stated that they were given little information and no training from the government. Some specified that they were told to disregard virtual learning all together while others were told to switch to WhatsApp without any specific support on how to operate specific platforms. Similarly, students mentioned not getting any support from the government or from their specific schools.

**“There was nothing from the government...it was private schools that knew we needed to come up with a solution for this, and that we should go virtual.” [A1]**

**“We did not get any help from the university. Students who personally reached out to teachers for guidance got a bit of help.” “This was a common complaint, that students did not understand [how to use these platforms].” [S5]**

### **3. Data collection, data access and storage**

The second set of questions in the survey were dedicated to exploring issues of data collection, access and storage within educational institutions. The first question in this regard was around the information collected by the school upon enrollment, to indicate the kinds of data that was at risk of breaches or violations and whether students and teachers were aware of what they were consenting to when disclosing their information. Unsurprisingly, the data taken by schools was extensive, as indicated by responses from students and parents as well as teachers and administrators. This information included student and parents’ names, email addresses, phone numbers, addresses, parents’ phone numbers, date of birth, blood groups, list of nationalities, national identification numbers of students and parents. These were generally mentioned by all respondents, followed by medical records, employment records of parents, bank account details and previous academic transcripts. A respondent also mentioned their school requiring vaccination certificates and COVID test reports.

**“We collected more data regarding students' access to smartphones, or even to a simple phone, whether parents could afford data packages, their household incomes, the students’ siblings that were studying...the literacy of the family.” [T1]**

**“If we had taken pictures of students during any sort of event we would, it would be like it’s our right to publish them. So we would just put them up on Facebook without even discussing it with them.” [A1]**

Specifically for virtual learning, students were asked for additional phone numbers and email addresses of family members. Students and parents were also asked if they were given any information about how their data is kept upon enrollment or during their time at school. 60% stated that they were given no information, while 20% stated that they didn’t know if they had been given information, while 16% stated that they were given some information on data collection and storage. Correspondingly, teachers and administrators were asked about who had access to the information given by students and their parents. 64% said that only administrators had access to the data, while 29% said administrators and teachers had access,

while 7% stated that only teachers had access. In interviews, both teachers and administrators stated that much of the collected data was stored in the form of hard copies, in registers, cupboards and closets with locks. This rather risky data storage technique suggests that data is constantly at the risk of being violated and breached in physical ways. Furthermore, without proper rules and regulations in place to protect, it is constantly subject to personal discretion and accountability.

**“Our clerk has his own cupboard and no one is allowed to touch it, and he has a lock on it. That's pretty much it.” [A1]**

**“So most data in schools is still stored in hard copies. So teachers have these registers that belong to the school...that they have to maintain for every single child.” [T1]**

This was further elaborated on in the interviews, where participants were asked about the ways in which this data is stored and the extent to which access is managed by the institutions. They were also asked whether the data is shared with any third parties, such as government departments and advertising agencies.

**“It is shared with the education ministry, and government departments that directly look into schools. Students’ names, grade levels, and how we track their academic performance is shared with third parties and donors, but nothing else.” [T1]**

This was coupled with concerns expressed directly by students during interviews. One student specifically mentioned feeling concerned about third party sharing and data access:

**“I want to know if my data is being given by the university to other institutions and how this data is being kept safe. How many people have access to this particular data and it isn’t just like data about what I’m studying and what my grades are. This is data about whether or not I’m using a certain service on campus or what time my classes are.” [S6]**



## 4. Privacy harms and risks

Students and parents / guardians were also asked a few questions about their fears and concerns about virtual learning and privacy. Additionally, they were asked about whether they had experienced any privacy harms while engaging in virtual learning. When asked about their general concerns about virtual learning, they stated many problems such as screen time, low internet connectivity, social isolation and learning loss but did not state fear of privacy violations or harms in their immediate responses. This can be attributable to privacy not being a key concern due to lack of information and awareness regarding this issue in the public domain, as well as it not being a priority due to more pressing concerns in Pakistan such as low internet connectivity and lack of teachers. Similarly, when asked about their privacy concerns, particularly whether they felt safe using online platforms, 51% said yes while 44% said they felt somewhat safe. 4% said they did not feel safe. However, when asked specifically whether they felt unsafe in online learning, several participants recalled events where they had suffered from “zoombombing” and been exposed to adult content while in online classes. In addition, students placed a lot of emphasis on the pressure to keep their cameras on and the fears of exposure and vulnerability associated with that.

**“Students are more hesitant to speak their minds [since the class is being recorded] because they don’t want to get in trouble. Some students don’t want their faces recorded on digital platforms.” [S1]**

**“Sometimes, because of our degrees, we say controversial stuff, because we are supposed to be questioning the status-quo. Sometimes I feel a little scared when the screen is being recorded, even if the video is going to be unlisted right.” [S6]**

For female respondents in particular - both students and teachers - gendered privacy harms were a key concern. Based on the incidences mentioned, it seems women are disproportionately affected by privacy breaches and are specifically targeted during such data violations. This is unsurprising given the patriarchal social context of Pakistan where women are subject to moral policing, threats and violence on a regular basis.<sup>62</sup>

---

<sup>62</sup><https://digitalrightsfoundation.pk/wp-content/uploads/2021/05/Moral-Policy.pdf>

**“There was an incident where a guy, through online classes, got a girl's email and harassed her using that over personal email.” [S2]**

**“A student shared his screen and his wallpaper was a screenshot of her profile picture. Some students even wrote inappropriate phrases on the teacher's screen through annotations. The teacher didn't really know what to do at that point since it was all new. I was really concerned with how easy it is for anyone to join the online sessions and hide behind a fake name.” [student survey response]**

**My number was on the learning pack and I trusted the photocopier but I did end up receiving a lot of wrong number calls. People would text or call me on WhatsApp and pretend to be my students; I had to put a filter up...” [teacher 4]**

**“My younger sister's (who is 15) class was zoom bombed by a guy who proceeded to pass crude remarks about the teacher and other girls in her class. It was very disturbing for a period of time.” [student survey response]**

This was also reflected in their recommendations for further change in virtual learning practices. When asked what they would like to see changed in the realm of online learning with regards to privacy, many mentioned that schools should not force students to keep their cameras on. Other recommendations were collected and are compiled below.

# Recommendations

## For schools/colleges/universities

- ▶ General awareness raising around campuses and by the management of institutions to bring greater understanding around the right to privacy and how it applies and affects all citizens of the country
- ▶ Institutions and workplaces should provide separate SIM cards and/or devices for professional or work-related engagements of their employees to protect their privacy in their off-duty hours and to also lessen the instances of harassment that female educators face
- ▶ Teachers should be trained properly, or given a course on how to prevent zoom bombing, hacking and virtual bullying.
- ▶ Written and accessible privacy policies in place which are transparently applied and contain accountability mechanisms in case there is a breach of privacy.
- ▶ Practice data minimization by collecting and recording data that is only strictly required.
- ▶ Students who belong to areas with limited connectivity are more vulnerable to privacy fallouts and institutions should be more cognizant of catering to all students.

## For education departments and administrators

- ▶ Adequate digital and technical literacy training to be imparted so that use of technology to stem impact from situations like COVID pandemic can be done safely and while maintaining a degree of personal privacy
- ▶ Inculcating the concept of consent and why it is important needs to be broached through awareness-raising programs in all institutions so that the importance of being responsible digital citizens can be highlighted

## **For the state**

- ▶ A lack of guidance was felt from the Higher Education Commission's end by educators, this should be raised with the Commission as they are the overarching authority for the education sector in Pakistan
- ▶ Government (HEC, School department) should roll out guidelines for virtual learning and then schools/university admins should make a policy according to that. Also, the policy must be explicitly communicated to teachers, students and parents by the educational institute
- ▶ Carry out extensive capacity-building for universities on how to use virtual learning tools in a safe and private manner.
- ▶ Draft a mandatory privacy policy to be implemented in all universities registered with the HEC.
- ▶ Adopt appropriate data protection legislation that takes into account the many risks and harms

## **For civil society actors**

- ▶ The virtual learning model did not consider the element of intrusiveness brought on by switching to from-home modes of communication which displace individual sense of privacy. Civil society must integrate these concerns into their larger advocacy for privacy.
- ▶ Organizations and activists working on education must advocate for privacy as part of student welfare.

## **Direct recommendations from consultations:**

- ▶ A model privacy policy should specifically address the concerns of teachers regarding recorded lectures. It should instruct educational institutes on how to prevent a privacy breach in terms of misuse of video lectures. It should have a component of ensuring a strict security standard whereby recorded data can only be accessible via passwords and cannot be downloaded by everyone. IP addresses should be monitored to ensure only students and teachers can access the data. Secondly, I feel a model policy should also set standards of informing the relevant persons regularly about the status of their data; if it is being accessed then by whom, the number of times it was accessed, till when will it remain accessible and when will it be deleted from the shared platform.
- ▶ The answer to a lot of these will be speculative because in my classes a lot of these issues didn't crop up because as an instructor I took care to ensure that wherever something privileged or sensitive was being discussed, it wasn't recorded but of course the students can be recording outside of zoom controls themselves too, but in that sense you don't moderate a discussion where there is this possibility of breach of confidentiality. Even in in person classes instructors in my uni in the past have been recorded without their knowledge and things they have said on religion etc have been quoted out of context and landed them in hot water. So it's definitely a risk and there ought to be policies against recording and sharing stuff discussed inside the classroom to maintain the sanctity of that space. But clear rules still need to be established to allow sharing of in class discussions in cases of harassment or ethnic/gender discrimination for sure. Tricky business. With Covid enforced online classes, uni admins were concerned with ensuring students turn up and pay the fees and have a semblance of normalcy in education continue. But that definitely put a lot of strain on teachers. That was not adequately considered, even in the more generous policy confines of my university. Double work, synchronous and asynchronous learning.
- ▶ Definitely as far as protection of privacy goes, the most important thing would be to create a culture of caring about it as a critical issue. There is far too much casualness in sharing information and storing information. Laws are probably the least significant deterrent in that regard simply because of ubiquity of privacy abuse. Hence institutes really ought to have rules and contingencies in place.

- ▶ Instructor empowerment to make choices on how much information to share and record, with adequate institute wide trainings on implications of privacy so an appropriate decision on particular pedagogical practices can be made with risk assessment

# Conclusion

Our survey findings, combined with our responses to the semi-structured interviews with a range of students and professionals in the education sector suggest that the state of privacy in the age of virtual learning in Pakistan is largely weak. This is true for privacy practices in all spheres, starting from government sector regulations, legal frameworks to protect data privacy, down to individual institutions and personnel managing data on a smaller scale. This is largely due to a lack of awareness and information about the importance of protecting data privacy, which was clear during our interviews with participants. Many were not concerned about privacy in general and those who were, were unable to articulate those concerns in the language of data privacy, rather mentioning individual cases of where they felt threatened or unsafe. This was particularly true for women, both as students and teachers, who shared daunting incidents of data violations and online harassment while they were engaged in virtual learning. It is imperative, therefore, to encourage wide scale awareness raising in the public domain on issues of privacy and data protection, particularly by calling on the state to take responsibility for the protection of student data and the protection of minors engaging in online learning platforms and using tools for virtual communication. As online spaces grow and reliance on these tools increases amid COVID-19, it is important to ensure that the privacy of individuals in the education sector is protected.



# References

1. "2019 State Of Edtech Privacy Report". 2019. Privacy.Commonsense.Org. <https://privacy.commonsense.org/resource/2019-state-of-edtech-privacy-report>.
2. "Allama Iqbal Open University". 2022. Aiou.Edu.Pk. Accessed January 4. <https://aiou.edu.pk/>.
3. "COVID 19 – TECHNOLOGY SUPPORT COMMITTEE: How Can Universities Prepare For The Transition To Virtual Instruction?". 2020. Hec.Gov.Pk. <https://hec.gov.pk/english/HECAnnouncements/Documents/nCoVirus/Approved-Working-Paper.pdf>.
4. "Covid-19 We Don'T Have To Choose Between Health And Privacy!". 2022. Accessed January 4. <https://www.coe.int/en/web/portal/covid-19-health-and-privacy>.
5. "Education: From Disruption To Recovery". 2022. UNESCO. Accessed January 4. <https://en.unesco.org/covid19/educationresponse#schoolclosures>.
6. "EDUCAUSE 2020 Student Technology Report: Supporting The Whole Student". 2020. <https://www.educause.edu/ecar/research-publications/student-technology-report-supporting-the-whole-student/2020/introduction>.
7. "HEC COVID-19 Policy Guidance Note 5: Online Readiness". 2022. Hec.Gov.Pk. Accessed January 4. <https://hec.gov.pk/english/HECAnnouncements/Documents/nCoVirus/Covid-19-Policy-Guidance-No.5-Online%20Readiness.pdf>.
8. "HEC Policy Guidance Series On COVID-19". 2020. Hec.Gov.Pk. <https://hec.gov.pk/english/HECAnnouncements/Documents/nCoVirus/Government-Directive.pdf>.
9. "How Does It Works? | COMSATS University Islamabad, Virtual Campus". 2022. Vcomsats.Edu.Pk. Accessed January 4. <https://vcomsats.edu.pk/about/how-it-works>.
10. "Massive School Data Breach Shows We Need Better Privacy Policies". 2021. Thehill. <https://thehill.com/opinion/technology/550959-massive-school-data-breach-shows-we-need-better-privacy-policies>.



11. "Privacy International's Comments On The Draft Prevention Of Electronic Crimes Act, 2015 (Pakistan)". 2015. Digitalrightsfoundation.Pk. [https://digitalrightsfoundation.pk/wp-content/uploads/2015/04/Prevention-of-Electronic-Crimes-Bill-2015-Legal-Analysis\\_0.pdf](https://digitalrightsfoundation.pk/wp-content/uploads/2015/04/Prevention-of-Electronic-Crimes-Bill-2015-Legal-Analysis_0.pdf).
12. "Shift To Online Learning Ignites Student Privacy Concerns". 2020. Iapp.Org. <https://iapp.org/news/a/shift-to-online-learning-ignites-student-privacy-concerns/>.
13. "The COVID-19 Pandemic Has Changed Education Forever. This Is How". 2020. World Economic Forum. <https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/>.
14. "Tracking The Global Response To COVID-19 | Privacy International". 2022. Privacyinternational.Org. Accessed January 4. <https://privacyinternational.org/examples/tracking-global-response-covid-19>.
15. "University Data Protection & Compliance: What You Need To Know | Virtru". 2022. Virtru. Accessed January 4. <https://www.virtu.com/blog/university-data-protection-2/>.
16. Annual Report 2021. Digital Rights Foundation. <https://digitalrightsfoundation.pk/wp-content/uploads/2021/03/Annual-Report-2020.pdf>.
17. Brodtkin, Jon. 2020. "Zoom Lied To Users About End-To-End Encryption For Years, FTC Says". Ars Technica. <https://arstechnica.com/tech-policy/2020/11/zoom-lied-to-users-about-end-to-end-encryption-for-years-ftc-says/>.
18. Cojocariu, V.-M., Lazar, I., Nedeff, V., Lazar, G. (2014). SWOT analysis of e-learning educational services from the perspective of their beneficiaries. *Procedia-Social and Behavioral Sciences*, 116, 1999–2003.
19. Dhawan, S. (2020) 'Online Learning: A Panacea in the Time of COVID-19 Crisis', *Journal of Educational Technology Systems*, 49(1), pp. 5–22. doi: 10.1177/0047239520934018.
20. Harris, Steve. 2020. "The Pandemic-Powered Rise Of Distance Learning". Orange Business Services. <https://www.orange-business.com/en/blogs/top-class-pandemic-powered-rise-distance-learning>.

21. Ilahi, Abiha, and Bilal Zaka. 2014. "Elearn Magazine: Elearning And Higher Education In Pakistan: What May Hamper It". Elearnmag.Acm.Org. <https://elearnmag.acm.org/featured.cfm?aid=2668882>.
22. Khan, Eesha Arshad. 2022. "The Prevention Of Electronic Crimes Act 2016: An Analysis". Shaikh Ahmad Hassan School Of Law. <https://sahsol.lums.edu.pk/law-journal/prevention-electronic-crimes-act-2016-analysis>.
23. Lemos, Robert. 2021. "Universities Face Double Threat Of Ransomware, Data Breaches". Dark Reading. <https://www.darkreading.com/attacks-breaches/universities-face-double-threat-of-ransomware-data-breaches>.
24. Littlefield, J. (2018). The difference between synchronous and asynchronous distance learning. <https://www.thoughtco.com/synchronous-distance-learning-asynchronous-distance-learning-1097959>
25. Mikkelsen, Daniel, Henning Solar, and Malin Strandell-Janssen. 2020. "Privacy, Security, And Public Health In A Pandemic Year". <https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/privacy-security-and-public-health-in-a-pandemic-year>.
26. O'Flaherty, Kate. 2020. "Beware Zoom Users: Here'S How People Can 'Zoom-Bomb' Your Chat". Forbes. <https://www.forbes.com/sites/kateoflahertyuk/2020/03/27/beware-zoom-users-heres-how-people-can-zoom-bomb-your-chat/>.
27. Olasile Babatunde Adedoyin & Emrah Soykan (2020) Covid-19 pandemic and online learning: the challenges and opportunities, Interactive Learning Environments, DOI: 10.1080/10494820.2020.1813180
28. Parkes, M., Stein, S., Reading, C. (2014). Student preparedness for university e-learning environments. The Internet and Higher Education, 25, 1–10. <https://doi.org/10.1016/j.iheduc.2014.10.002>
29. Raj, Aaron, and Aaron Raj. 2021. "Education Sector Hardest Hit By Ransomware In 2020 - Techhq". Techhq. <https://techhq.com/2021/07/education-sector-hardest-hit-by-ransomware-in-2020/>.
30. Schleicher, Andreas. 2020. "The Impact Of COVID-19 On Education: Insights From Education At A Glance". Oecd.Org. <https://www.oecd.org/education/the-impact-of-covid-19-on-education-insights-education-at-a-glance-2020.pdf>.

31. Siddiquei, Nabia Luqman, and Ruhi Khalid. 2017. "Emerging Trends Of E-Learning In Pakistan: Past, Present And Future". Academia.Edu. [https://www.academia.edu/39702296/Emerging\\_Trends\\_of\\_E\\_Learning\\_in\\_Pakistan\\_Past\\_Present\\_and\\_Future](https://www.academia.edu/39702296/Emerging_Trends_of_E_Learning_in_Pakistan_Past_Present_and_Future).
32. Singh, V., Thurman, A. (2019). How many ways can we define online learning? A systematic literature review of definitions of online learning (1988-2018). *American Journal of Distance Education*, 33(4), 289–306.
33. Song, L., Singleton, E. S., Hill, J. R., Koh, M. H. (2004). Improving online learning: Student perceptions of useful and challenging characteristics. *The Internet and Higher Education*, 7(1), 59–70.
34. Wilson, Jim. 2022. "Up To 2 Million People Affected By Data Breach At Indian E-Learning Platform". Safetydetectives. Accessed January 4. <https://www.safetydetectives.com/blog/edureka-leak-report/>.



DigitalRightsFoundation