INTERNET FREEDOM FOUNDATION
internetfreedom.in policy@internetfreedom.in +91 011 47640713

By Email
Without Prejudice

To,
Priyank Kanoongo,
Chairperson, National Commission for Protection of Child Rights (NCPCR),
5th Floor, Chanderlok Building,36 Janpath,
New Delhi, Delhi 110001
Email ID: cp.ncpcr@nic.in

Dated: February 15, 2023 IFF/2023/006

Hon'ble Chairperson,

***Re: Representation to the NCPCR on the breach of personal data of millions of teachers and school students by the Digital Infrastructure for Knowledge App (DIKSHA)***

1. The Internet Freedom Foundation (IFF) is an Indian member-supported non-profit organisation that ensures technology advances with fundamental rights, born out of the SaveTheInternet.in movement for net neutrality. We work across a wide spectrum of issues, with expertise in free speech, electronic surveillance, data protection, net neutrality and innovation; we aim to champion privacy protections, digital security, and individual freedoms in the digital age.

**Factual Background**

2. We want to raise our concerns surrounding the data collection by the Diksha App, an EdTech app owned and operated by India's Education Ministry.[1] According to a report dated Jan 23, 2023 published by Wired, owing to the application, millions of children's and teachers' personally identifiable information continues to be in the public domain. The complete names, contact information, and email addresses of more than 1 million instructors are stored in files on the unprotected server, along with information concerning over 600,000 students.[2] A report by Human Rights Watch ('HRW') dated May 25, 2022, named Diksha among 21 other apps which were guilty of enabling third-party companies to access children's precise location data, potentially enabling these companies to analyse, trade, and monetize this information.[3]

3. The application, though launched in 2017, gained increased importance between the period 2020-2022, when it became the primary platform for delivering online education to students. It offers lessons, textbooks, homework, and other educational material for grades 1 to 12. Presently,

[1]Department of School Education & Literacy Ministry of Human Resource Development, India Report Digital Education: Remote Learning Initiatives Across India June 2020, Delhi: Digital Education Division, Department of School Education & Literacy, Ministry of Human Resource and Development, 2020, https://www.education.gov.in/sites/upload_files/mhrd/files/India_Report_Digital_Education_0.pdf (accessed February 9, 2023).
[2]Vittoria Elliot and Dhruv Mehrotra, *A major app flaw exposed the data of millions of Indian students*, Wired, January 23, 2023, https://www.wired.com/story/diksha-india-education-app-data-exposure/ (accessed February 8, 2023).
[3]Andrea Devia Nuño, *"How dare they peep into my private life?"*, Human Rights Watch, May 25, 2022, https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments (accessed February 8, 2023).

the application has 16,62,11,232 enrolments.[4]

4. The HRW report revealed that Diksha collects children's precise location data, including the date and time of their current location and their last known location. This crucial information is not disclosed in the app's privacy policy. An app specific analysis on Diksha by HRW also brought to the fore that Diksha was collecting and transmitting children's Android Advertising IDs (AAIDs) to Google through two Software Development Kits (Google Firebase Analytics and Google Crashlytics) embedded in the app.[5]

5. The State Government of Uttar Pradesh set quotas and pressurised teachers to get students to download the impact without gauging the after-effects of such a move and leaving children with no choice but to download the app in order to continue their education.[6] A report by the Human Rights Watch titled "Indian Government App Exposed Children's Personal Data: A Rights-Respecting Data Protection Law Urgently Needed" aptly commented that the Indian government's proposed data protection law 2019 fails to protect children against inappropriate use of data by vendors, and insecure data transfer/storage, among other things.[7] The draft Digital Personal Data Protection Bill 2022, in its current format, continues to suffer from inadequacies, rendering it incapable of protecting the sensitive personal data of children.

**Our Concerns**

6. The breach violates the students' fundamental right to privacy, as upheld by the Supreme Court in the *K.S. Puttaswamy v. Union of India*.[8] Significantly, the judgement highlighted the need to secure children's right to privacy, bearing in mind that minors lack the legal capacity to give consent. Hence, if necessary measures are not taken to protect the personal information of children, it would stand in violation of the Puttaswamy decision.

7. Additionally, the Union Government, in 2005, had accepted two Optional Protocols to the United Nations Convention on the Rights of the Child (UNCRC).[9] As a result, India endeavours to protect children from all forms of exploitation. To quote Article 16 of the UNCRC:

> *i) No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honor and reputation.*
> *ii) The child has the right to the protection of the Law against such interference or attacks.*

[4]https://diksha.gov.in.
[5]Diksha: App Analysis, https://features.hrw.org/features/StudentsNotProducts/files/privacy_snapshots/Privacy%20Snapshot%20-%20India%20Diksha.pdf (accessed February 8, 2023).
[6]Ishita Bhatia, *Remote learning: UP sets target, tells each govt teacher to convince 10 students to download Diksha app*, The Times of India, November 18, 2020, http://timesofindia.indiatimes.com/articleshow/79268507.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst (accessed February 8, 2023).
[7] Hye Jung Han, *Indian Government App Exposed Children's Personal Data*, Human Rights Watch, January 27, 2023, https://www.hrw.org/news/2023/01/27/indian-government-app-exposed-childrens-personal-data (accessed February 8, 2023).
[8](2019) 1 SCC 1.
[9]United Nations Human Rights, Convention on the Rights of the Child, https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child (accessed February 9, 2023).

8. The collected information can leave several students and teachers vulnerable to fraud and identity theft, as individuals do not change their personal information, especially email addresses and phone numbers, over such a short period.[10] Unbeknownst to the parties tracked, complex algorithms are in use to sweep through the data pool and bring to use the data collected in many unimaginable ways.[11] The children and their parents are deprived of the opportunity to make informed decisions about such data sharing.

9. A report by the FirstPost on October 25, 2015, highlighted how sexual predators, on procuring children's sensitive information such as their names and contact details - which was freely available on a university's website - began to contact and lure them under the guise of offering career advice.[12] In an interview dated July 12, 2021, conducted by the New Indian Express, a technology expert highlighted that in instances of such data breaches, there is also a possibility of students' contact numbers being uploaded on pornographic websites.[13] Multiple reports relating to the critical misuse of personal data to commit crimes against children are frequently carried in the press.[14] These incidents highlight the risks posed by compromising children's right to privacy.

**Recommendations**

10. Given the serious personal data breach and its impact on several students, we urge the Commission, as empowered by Section 13(1) and Section 14(2) of the Commissions for Protection of Child Rights Act, 2005, read with Section 24 of the Act, to consider the following:

    a. Initiate an inquiry about gaining access to students' personal information and into the alleged nature of data collected by the app.

    b. Recommend remedial measures to safeguard children's data to prevent the leakage of personal data henceforth. IFF believes that the following enactments offer key insights into safeguarding children's sensitive data and would be beneficial to the Commission to frame the remedial measures:

        i. General Data Protection Regulation (GDPR): Article 5 of the GDPR lays down the principles vis-a-vis processing, storing, managing and collecting personal data.

---

[10] *Cyberbullying: What is it and How to stop it*, UNICEF, February 2023, https://www.unicef.org/end-violence/how-to-stop-cyberbullying (accessed February 8, 2023).

[11] Janna Anderson, Lee Rainie and Emily A. Vogels, *Experts Say the 'New Normal' in 2025 Will Be Far More Tech-Driven, Presenting More Big Challenges,* Pew Research Center, February 18, 2021, https://www.pewresearch.org/internet/2021/02/18/experts-say-the-new-normal-in-2025-will-be-far-more-tech-driven-presenting-more-big-challenges/ (accessed February 8, 2023).

[12] A Saye Sekhar, *Hyderabad: Sex predator uses exam data to trap, sexually exploit and blackmail girl*, FirstPost, October 25, 2015, https://www.firstpost.com/india/hyderabad-sex-predator-uses-exam-data-to-trap-sexually-exploit-and-blackmail-girls-2481548.html (accessed February 8, 2023).

[13] N Dhamotharan, *Tamil Nadu school education department officials selling students' data?*, New Indian Express, July 12, 2021, https://www.newindianexpress.com/states/tamil-nadu/2021/jul/12/tamil-nadu-school-education-department-officials-selling-students-data-2328770.html (accessed February 8, 2023).

[14] *Over 400% rise in cyber crime cases against children in 2020: NCRB data*, November 14, 2021, https://www.business-standard.com/article/current-affairs/over-400-rise-in-cyber-crime-cases-against-children-in-2020-ncrb-data-121111400320_1.html (accessed February 15, 2023).

ii. The Family Educational Rights and Privacy Act, 1974 (FERPA): This federal law passed by the United States of America provides schools guidelines to manage and use student data. Moreover, FERPA stipulates that third parties could gain access to a child's personal data only if the child's parent consents to the disclosure.

c. Effectively implement the remedial measures by drafting comprehensive guidelines to sensitise schools, educational institutions, and other stakeholders to protect students' sensitive data.

Therefore, in light of students' privacy and personal data being at stake, we earnestly urge the NCPCR to consider our application and look into the matter. We value the opportunity for any further requests for information, inputs or clarifications and remain available for meetings.

Kind regards,

Prateek Waghre,
Policy Director,
Internet Freedom Foundation
anushka@internetfreedom.in