Mendoza Law, LLC

1000 University Ave., W. Suite 222
Saint Paul, MN 55104
651-330-8062 (Main)
www.mendozalawoffice.com

By: Kaylee Kruschke, Esq.
Direct Dial: 651-502-2885
kaylee@mendozalawoffice.com
and
Jessica D. Schatz

December 4, 2020

Protecting Children's Privacy During COVID-19

When COVID-19 cases began to rise in the U.S. in mid-March, educators moved swiftly to transition their classrooms into the virtual world by using video conferencing platforms. While this strategy helped maintain the safety of students' physical health, it also raises questions about their privacy rights. With COVID-19 still raging, many classrooms continue to operate virtually, and educators and parents need to understand the privacy implications posed by the virtual platforms their students and children are using daily.

In October, the Center for Democracy and Technology released results from a study surveying K-12 teachers and parents from public schools across the United States. The survey showed that 80 percent of teachers have not been asked about student data privacy by parents or students since COVID-19 began. Only 43 percent of parents said they knew that their child's school had a technology plan addressing student privacy and security issues.

One of the best-known video conferencing platforms, Zoom, provides schools the option to create K-12 Accounts that schools may provision to student users. When a school subscribes to Zoom K-12 Accounts, Zoom allows the school to determine how personal information is processed. For example, the school can determine if meetings can be recorded and where the recording is stored and is responsible for obtaining any necessary consent from participants. Additionally,

the processing of students' personal information by the school through Zoom is determined and administered by the school under the school's privacy policies. Zoom advises parents to contact their child's school if they have questions regarding any of the school's privacy policies in relation to the school storing students' personal information collected through Zoom.

On Zoom's side of the equation, when schools subscribe to K-12 Accounts, Zoom receives students' personal information and maintains that personal information at the direction of the students' school. Zoom also states that it does not use any personal information from students for any other purposes except as permitted by applicable law and its agreement with each school. The most important aspect of Zoom's K-12 Account policy is that Zoom commits to only using personal information collected about student users of K-12 Accounts as needed to deliver the functionality of the Zoom platform, operate the business, including to enhance or improve Zoom services, and as directed for by the child's school. That means Zoom does not sell students' personal information, use students' personal information to deliver behavioral advertising, or allow third-party advertising or analytics on Zoom's product pages.

While Zoom's policy for K-12 Accounts seems protective of student privacy rights, the unfortunate aspect is that students are not allowed to create a K-12 Account on their own. If a school chooses not to subscribe to K-12 Accounts, students using Zoom under a personal account do not gain the privacy protections provided by Zoom's K-12 Account policy. Instead, those students are subject to Zoom's general account user privacy policy. With general user accounts, Zoom uses cookies and gives information to advertising services. Users can opt-out of their personal data being sold, but this is not the default. From a student privacy standpoint, this is concerning because Zoom, and many of the other video

platforms schools are using to operate virtual classrooms, take, store, and often sell user data to entities in the marketing industry.

Considering this, there are three things parents should consider doing to help protect their children's privacy when it comes to virtual classrooms. First, parents should ask whether their children's school has vetted the company providing video platform services to operate virtual classrooms and what the contract between the school and the video platform service says about how student personal information is used and handled.

Second, some companies have also agreed to sign the Student Privacy Pledge. This pledge requires companies to commit to 14 legally binding obligations, including not selling students' personal information and not collecting or using students' personal information for anything other than what is needed for educational purposes. Parents should research the Student Privacy Pledge and determine if the platform their children's school uses has agreed to sign the pledge.

Third, parents should talk to their children about the importance of protecting personal information and discuss things like not sharing passwords or sharing other private information via video chat.

While we all adjust to the new way of living COVID has brought, it is important to be cognizant of privacy issues when it comes to children and their daily use of virtual classrooms.