Safeguarding Student Privacy in Schools

by Miranda Doyle
(she/her)
District Librarian,
Lake Oswego School District
doylem@loswego.k12.or.us
@MsMintheLibrary

Miranda Doyle (she/her) is a District Librarian at Lake Oswego School District. Before she switched to school libraries, Miranda was a Young Adult Librarian and then a Branch Manager for the San Francisco Public Library. She is currently serving as a member of the Oregon Intellectual Freedom Committee. In her spare time, Miranda enjoys running, kayaking, and learning Brazilian jiu jitsu.

Schools have always collected data on their students—everything from grades and test scores to information about behavior and medical issues. Beginning in March 2020, however, the potential for unwanted sharing of student information exploded. Most schools without existing 1-to-1 technology programs, where every student is assigned a digital device, scrambled to hand out laptops, Chromebooks, or iPads to students. Schools also tried out and adopted digital teaching tools such as Google Classroom, Canvas, Clever, Pear Deck, Flipgrid, Edpuzzle, Screencastify, Explain Everything, Kahoot!, GoNoodle, and many others. The COVID-19 pandemic pushed many schools fully online. Now, with schools back to in-person learning, school activities still often depend on the use of these digital devices and tools.

Parents and guardians of preschoolers have some power to limit how much data children share. However, after these children enter kindergarten, they are usually required to use online learning platforms to access and turn in assignments. Even if schools allow parents and guardians to opt their children out of taking a device home or using specific apps, opting out can make it very difficult for students to participate in classes. For example, if students use Chromebooks and teachers use Google Classroom to post assignments, an opted-out student would not be able to take part in learning activities or even know what homework they're responsible for. A study conducted in the summer of 2021 concluded that more than one in three parents said they were "very concerned" about security and privacy issues around their student's data (Klein, 2021b).

School administrators must consider the digital rights of these students and families as they choose resources. It's also important for parents, teachers, school librarians, and the broader community to know the types of data that schools and their third-party vendors collect, and what they can do to better protect that data.

Multiplying Devices and Apps

Before the pandemic, only some schools provided a device for each student to take home. Now most do. A February 2021 survey by the EdWeek Research Center found that 42 percent of schools gave each elementary student a digital device before the pandemic, but that number doubled to 84 percent by the middle of the 2020–21 school year (Klein, 2021a). The same survey found that 90 percent of middle and high schools issued 1-to-1 devices. As schools increasingly use cloud-based services such as Google Classroom and Google Drive, they are turning over huge amounts of information to technology companies.

In addition, many school districts now use threat detection and prevention software to monitor online activity (Herold, 2019). Private companies offer schools 24/7 monitoring and alerts, searching student emails, files, and social media for keywords and images.

Why worry about data collection and privacy? For one, this collected information can be used in ways that are inequitable and damaging. In one horrifying example, a school district in Florida shared student data with the police department, including grades, disciplinary histories, and whether the students had experienced trauma (Lieberman, 2021). The police department then used the data to compile "a secret list of middle and high school students it deems as potential future criminals."

In addition, data leaks and ransomware attacks on schools are common. One investigation found children's personal information, directly from school files, for sale on multiple websites (Collier, 2021). School districts, along with hospitals and other large organizations, have become a target for hackers. Some school districts have paid hackers to restore access to their student information systems, or refused to pay. Locally, Portland's Centennial School District experienced a data breach and discovered that district data was posted online | (Ramakrishnan, 2021).

Third-Party Vendors and Student Privacy

Schools often contract with multiple third-party vendors for cloud-based software and services to track student attendance, test scores, educational plans, student work samples, health information, and other data. Teachers also sign their classes up for educational apps and websites—classroom social media sites, typing or math practice, ebook providers, and much more. Districts should develop and adopt privacy policies, and should evaluate new and existing online services to make sure they don't share student data or collect more information than is necessary.

However, even school districts with a thorough process for investigating privacy policies must depend heavily on vendor claims. Districts aren't often able to scrutinize the company's actual practices. For example, many school districts now issue Chromebooks to students and enroll them in Google Apps for Education, which includes Google Docs, Classroom, and Drive. While these tools are useful (and the basic version is free to schools), some have questioned how Google uses children's data. Google says it does not collect information on students for advertising purposes, but that may not always be true. In 2015, the Electronic Frontier Foundation filed a complaint with the Federal Trade Commission alleging that Google was tracking students and building profiles on them. Google claims to have changed its practices in response (Cope, 2016).

In September 2019, Google paid a $170 million fine for violating the federal Children's Online Privacy Protection Act (COPPA) after regulators said that Google-owned YouTube “knowingly and illegally harvested personal information from children and used it to profit by targeting them with ads” (Singer & Conger, 2021). So, even companies that have strong written privacy policies might not always follow their own rules.

Video Platforms in Schools

In March 2020, many schools started conducting classes over video platforms such as Zoom or Google Meet. This raised new privacy concerns. Because there was little advanced planning, most schools—and school librarians, who often assisted with the transition—jumped to video platforms without time to vet policies, procedures, and tools. Public libraries also dealt with these issues as they implemented online library programming such as author visits, trivia nights, and guest speakers. Now, even with in-person events returning, video meetings are still used—for parent conferences, for example.

Many questions surround schools’ use of video conferencing platforms. For example, what data do Zoom and other platforms collect about students? How secure are these platforms? Where are the videos stored? How long will schools keep them? Screen captures made by students or other participants in a meeting can also violate privacy, as when a student records and shares a clip. Teacher trainings have also been recorded by an attendee—this issue surfaced in Oregon when clips from a Beaverton School District Zoom meeting appeared in the news and on social media and created an uproar (Marnin, 2021). Additionally, teachers and other school staff are faced with the issue of seeing or hearing problematic things while on a Zoom call. While teachers are mandated to report abuse or neglect, there is also the potential for over-policing, as when police went to a Black seventh-grader’s house because he was playing with a Nerf gun during an online art class (Peiser, 2020).

Privacy in the School Library

School libraries also need to be concerned about their own data collection. For example, school librarians can ensure that library circulation records aren’t stored in their circulation system forever, and that notes left on patron records are deleted regularly. School libraries should make sure that their ebook and database providers follow laws about collecting personal information about students and their reading or research habits. When the Statewide Database Licensing Advisory Committee chooses databases for libraries in Oregon, for example, privacy is an important criterion in the selection process.

Print books and materials aren’t exempt from privacy issues. For example, should school libraries send overdue notices directly to parents? Does this inhibit students who might otherwise borrow books on sensitive topics? School libraries may also keep a student’s checkout records in their circulation software and ebook platform even after items are returned. What if a parent, teacher, principal, or law enforcement officer comes into the library to ask which books a student has borrowed? School libraries often deal with such privacy concerns differently from public libraries.

Schools, parents, guardians, and concerned community members can help address these issues using a variety of strategies. They can learn more about the federal and state laws regarding data collected about children. The Children’s Online Privacy Protection Act (COPPA) and the Family Educational Rights and Privacy Act (FERPA) guide the manner in which service providers and schools can use or release student information. Schools can write or strengthen privacy policies with input from all the stakeholders. Schools can choose third-party vendors who do not sell student information or track students for advertising purposes. This might mean paying for digital services, so that companies earn revenue from subscriptions rather than from collecting and selling student data. Sometimes schools and libraries can choose which records to collect, and decide not to store personally identifying information beyond the minimum required. Families and community members can ask which services and tools students use in class.

All of these steps are important in making sure student data is as secure as possible, and that it is used only to advance educational goals.

References

Collier, K. (2021, September 10). Hackers are leaking children's data—and there's little parents can do. *NBC News*. https://tinyurl.com/2t2ujvns

Cope, J. G. (2016, October 6). Google changes its tune when it comes to tracking students. *Electronic Frontier Foundation.* https://tinyurl.com/2p87p4s6

Herold, B. (2019, May 30). Schools are deploying massive digital surveillance systems. The results are alarming. *Education Week.* https://tinyurl.com/yr5j9vwb

Klein, A. (2021a, April 20). During COVID-19, schools have made a mad dash to 1-to-1 computing. What happens next? *Education Week.* https://tinyurl.com/2p8nx3nh

Klein, A. (2021b, November 16). Ed tech usage is up. So are parent privacy concerns. *Education Week.* https://tinyurl.com/bdfk2edx

Lieberman, M. (2021, February 23). Using student data to identify future criminals: A privacy debacle. *Education Week.* https://tinyurl.com/nsbtjb9z

Marnin, J. (2021, May 28). Twitter outraged over teacher telling educators to embrace anti-racist thinking or be fired. *Newsweek*. https://tinyurl.com/4ead4huw

Peiser, J. (2020, September 8). A Black seventh-grader played with a toy gun during a virtual class. His school called the police. *Washington Post.* https://tinyurl.com/yc3rc233

Ramakrishnan, J. (2021, April 26). Centennial schools to close for 2 days after hackers breach school technology systems. *The Oregonian*. https://tinyurl.com/3tv83drp

Singer, N., & Conger, K. (2021, August 10). Google is fined $170 million for violating children's privacy on YouTube. *The New York Times.* https://tinyurl.com/2p9dma9p