Parents: Raise Your Hand and Ask Schools How They Protect Student Data

By Sara Collins, Tyler Park, and Amelia Vance

As you send your child off to start a new school year, you may have questions about how your child's teachers are using new technologies, such as tablets, computers, apps, or online learning platforms. What kind of information will they collect, and how will it affect child's privacy? With all of the new educational technology in classrooms, it can be hard to know what questions to ask. Here are the 7 most important questions that parents should ask about student privacy during this school year.

1. Which websites, services, and apps will my child's classroom use this year?

Parents frequently report that education technology in the classroom has improved how their child learns.[1] When properly implemented, technology and data can be powerful tools for delivering high quality education. But your child's school should tell you about what technologies (apps, websites, or online services) your child will be using, and how they have vetted those services to ensure they are safeguarding your child's privacy. Many schools send a letter at the beginning of the school year with a list of the apps that will be used; others post the apps used on the school's website, along with the kinds of data each of those apps collect.[2] If your child's school hasn't done so, request this information—and ask questions about any descriptions that don't make sense.

2. How does my school handle directory information?

"Directory information" is a legal term for the kind of information you might find in a PTA directory or yearbook, including students' and parents' names, addresses, phone numbers, email addresses, participation in activities and sports, and dates of attendance.[3]

Children at school by Lucélia Ribeiro (Lupuca), Flickr, CC BY-SA 2.0

Most of the time, under federal law, student information—such as grades, discipline records, or medical visits—cannot be shared with anyone without your consent. However, "directory information" is an exception. Schools can choose to post this information online, or share it with anyone (parents must be given the right to opt out). For this reason, directory information can sometimes be misused. In one recent case, schools in Virginia shared directory information with a political candidate, who then used it to send students text messages about registering to vote.[4]

Parents should know that schools are required to notify them every year about what information they consider to be directory information, and schools can choose to limit who can receive directory information —for example, by promising in their annual notice that they will never provide information for a profit-making activity, or giving parents the right to only allow the disclosure of certain types of information.[5] In order to make an informed decision about whether to opt out, ask your school how they define directory information, and with whom it is shared.

3. What is my school's approach to school safety, and what does it mean for my child's privacy?

In the wake of the Parkland school shooting in February 2018, many schools introduced new measures to help identify threats to the school, potential self-harm, or cyberbullying. These might include social media monitoring, digital video surveillance linked to law enforcement, or tracking students' online activities on personal or school-issued devices, raising privacy concerns.[6] These measures may help protect students, but

surveillance can also impact students' autonomy and sense of freedom if there are not appropriate measures in place to guide their use. Ask what steps your school has taken to protect school safety, how the school has built privacy protections, and the school's process when it identifies a student's activity as threatening or problematic.[7]

4. Does my child's school administer surveys?

You should know what information your child is being asked to provide in school, especially when that information does not or only tangentially relates to what they need to learn. When students take surveys in school, the federal Protection of Pupil Rights Amendment (PPRA) applies.[8] The PPRA establishes a parents' right to inspect school surveys before the survey is given. If a survey asks about certain sensitive topics—like family income, religion, political beliefs, or anti-social behaviors—the PPRA requires even more: parents must be given the opportunity to opt their child out of taking the survey.

The Department of Education recently released guidance regarding administration of third-party surveys in schools, such as the pre-survey on college admissions exams like the SAT and ACT.[9] Websites that help students choose career paths or get scholarships, while helpful for students, may not have any restrictions on sharing the sensitive data they collect. That means that the student may be targeted for inappropriate marketing, discriminated against, or even have their data revealed to data brokers.[10] The PPRA requires districts to have policies about surveys given in schools, and they must consult with parents about these policies. Ask your school about their policy and how they will share surveys with your child throughout the school year.

5. What are the rules for recording devices in my child's school?

Be aware of your school's policies about the use of recording devices as they can be beneficial but also often raise privacy questions, such as who is listening in, and why. In an effort to protect student privacy, some schools and state legislatures have banned the use of recording devices (including using cell phones to record) in schools, with mixed results.[11] Parents and students in Maine, Virginia, and Illinois have encountered legal issues after using recording devices in the classroom, with one parent even facing felony charges for putting a recording device in her daughter's backpack to identify school bullies.[12]

At the same time, recording in classrooms can be important for students with disabilities, and is often included as part of Individualized Education Programs. AngelSense, for example, is a GPS tracking device designed for autistic children, and has a "listen in" feature that allows parents to hear what is going on around their child. In response to privacy concerns, AngelSense worked with districts to create an agreement disabling the "listen in" feature during school hours while still allowing parents retain the essential GPS capability.[13]

Computer Security - Padlock by Blue Coat Photos, Flickr, CC BY-SA 2.0

6. How is my child's information secured?

Last fall, four small school districts were targeted by malicious hackers that used student data to text death threats to parents and students and attempt to convince the districts to pay a ransom.[14] Although schools might not store financial information, like credit card or social security numbers, schools do hold data that is extremely sensitive and must be kept safe. Ask your school how it is protecting the safety of your child's information. The Department of Education provides a checklist of data security issues for schools you can use to create questions, and FPF has a list of seven security questions to ask about ed tech platforms.[15]

7. How does the school train teachers and staff to protect student information?

Most data breaches are caused by human error, such as clicking a link in a phishing email or choosing a weak password.[16] Often, these errors

Insect Exhibit in the Barrett Discovery Lab by projectdiscovery, Flickr, CC BY-SA 2.0

result from insufficient training. Almost half of districts in the US have fewer than 1000 students, and they often do not have the budget or expertise to implement sophisticated privacy and security measures.

Even if state laws require schools to secure student data, it is difficult for schools to comply with legal requirements without funding and training. Utah is the only state that requires that educators take an annual privacy course for relicensure, and also requires that all school employees with access to cumulative records have a data confidentiality training (check out their free Canvas course and YouTube training!), though many other states and districts—both big and small—have found ways to build a culture of privacy.[17] The Future of Privacy Forum's FERPA|Sherpa website also has useful training resources for schools and teachers.[18] Ask your school what training they conduct throughout the year to protect your child's information. If they aren't doing training right now, point them towards these resources or other amazing groups like the Department of Education's Privacy Technical Assistance Center (PTAC), the Student Data Privacy Consortium (SDPC), or the Consortium for School Networking (CoSN) for help.[19]

Your school may not have answers to all of these questions. This does not necessarily mean that there is cause for concern; for many districts, privacy and security are in competition with other vital priorities such as improving educational outcomes, safety, or graduation rates. Nevertheless, caring for your child's data should be important to your school. Back-to-school is a perfect time to ask questions about technology and data use in schools. By asking the right questions, you can be informed about the policies and procedures being used to protect your child's information and be in a position to speak up and demand meaningful privacy safeguards.

Resources

1.2016 Parent Survey, Amelia Vance, Future of Privacy Forum (Dec. 8, 2016) https://fpf.org/2016/12/08/2016-parent-survey/
2. FERPA-Approved Apps List, Denver Public Schools (last visited Sep. 7, 2018) https://atm.dpsk12.org/ferpaapproved.aspx.
3. Frequently Asked Questions, U.S. Department of Education, (last visited Sep. 7, 2018) https://www2.ed.gov/policy/gen/guid/fpco/faq.html.
4. Virginia House Approves Bill to Shield Student Contact Info, Graham Moomaw, Richmond Times-Dispatch (Feb. 7, 2018) https://www.richmond.com/news/virginia/government-politics/general-assembly/virginia-house-approves-bill-to-shield-student-contact-info-from/article_70eb1955-dedb-521b-b955-95a15f139174.html.
5. 33 Ohio Rev. Code 3319.321, http://codes.ohio.gov/orc/3319.321; 2017-2018 Annual Notice - Survey, Records, Curriculum, Privacy, and Related Rights, Fairfax County Public Schools, (last visited Sep. 7, 2018) https://www.fcps.edu/sites/default/files/media/forms/2017-18%20Complete%20Packet%20K-8_0.pdf.
6. The Secretive Industry of Social Media Monitoring, Malena Corrolo (last visited Sep. 7, 2018) http://projects.csmonitor.com/socialmonitoring.
7. Fair Information Practice Principles, Federal Trade Commission, (archived Sep. 11, 2007) https://web.archive.org/web/20131110022137/http://www.ftc.gov/reports/privacy3/fairinfo.shtm; Targeted: A Family and the Quest to Stop the Next School Shooter, Bethany Barnes, The Oregonian (June 24, 2018) https://www.oregonlive.com/expo/news/erry-2018/06/75f0f464cb3367/targeted_a_family_and_the_ques.html?curator=MediaREDEF.
8. 20 U.S.C § 1232(h) (2018) https://www.law.cornell.edu/uscode/text/20/1232h.
9. Dept of Ed: Parents, Not Minor Students, Must Consent to College Admissions Pre-Test Surveys and Data Sharing, Amelia Vance, Future of Privacy Forum (May 24, 2018) https://fpf.org/2018/05/24/dept-of-ed-parents-not-minor-students-must-consent-to-college-admissions-pre-test-surveys-and-data-sharing/.
10. Students With Disabilities Sue ACT Over Release of Personal Information, Catherine Gewertz, Education Week (Aug. 7, 2018) http://blogs.edweek.org/edweek/high_school_and_beyond/2018/08/students_with_disabilities_sue_act_over_release_of_personal_information.html ; For Sale: Survey Data on Millions of High School Students, Natasha Singer, New York Times (July 29, 2018) https://www.nytimes.com/2018/07/29/business/for-sale-survey-data-on-millions-of-high-school-students.html.
11. Policy over use of video recordings in classrooms to be reviewed, Paul Feely, New Hampshire Union Leader (Dec. 10, 2015) http://www.unionleader.com/Policy-over-use-of-video-recordings-in-classrooms-to-be-reviewed.
12. Federal Court: Maine Parents Can't Record Son's School Day, Alanna Durkin Richer, Associated Press (Mar. 27, 2018) http://bangordailynews.com/2018/03/27/news/midcoast/federal-court-maine-parents-cant-record-sons-school-day/; Charges Against Mom who Tried to Record Bullying Are Dropped, Jason Hanna, Alison Kosik and Darran Simon, CNN (Nov. 29, 2017) https://www.cnn.com/2017/11/29/us/virginia-mother-bullying-arrest/; This 13-year-old Boy Recorded his Talk with the Principal — now He's Being Charged with an Eavesdropping Felony, Erin Donnelly, Yahoo Lifestyle (June 21, 2018) https://www.yahoo.com/news/13-year-old-boy-recorded-talk-principal-now-hes-charged-eavesdropping-felony-163354136.html.
13. AngelSense (last visited Sep. 7, 2018) https://www.angelsense.com/; Testimony and Statement for the Record of Amelia Vance, Hearing on "Protecting Privacy, Promoting Data Security: Exploring How Schools and States Keep Data Safe" Before the House Committee on Education and the Workforce, page 6, (May 17, 2018) https://edworkforce.house.gov/uploadedfiles/testimony_vance_5.17.18.pdf.
14. 'Dark Overlord' Hackers Text Death Threats to Students, Then Dump Voicemails From Victims, Joseph Cox, Daily Beast, (Oct. 5, 2017) https://www.thedailybeast.com/dark-overlord-hackers-text-death-threats-to-students-then-dump-voicemails-from-victims.
15. Data Security Checklist, Privacy Technical Assistance Center, (last visited Sep. 7, 2018) https://nces.ed.gov/programs/ptac/pdf/ptac-data-security-checklist.pdf; Brenda Leong, Seven Basic Security Checks for Evaluating Educational Platforms, Future of Privacy Forum (Nov. 7, 2016) https://fpf.org/2016/11/07/seven-basic-security-checks-evaluating-educational-platforms/.
16. Data Indicates Human Error Prevailing Cause of Breaches, Incidents, Mahmood Sher-Jan, International Association of Privacy Professionals (June 26, 2018) https://iapp.org/news/a/data-indicates-human-error-prevailing-cause-of-breaches-incidents/; Human Error to Blame in the Vast Majority of Education Data Breaches, Mark Satter, EdScoop, (May 18, 2018) https://edscoop.com/human-error-majority-k-12-education-data-breaches.
17. Utah Board Rule R277-487 and the Utah Student Privacy Act, respectively, require that educators take the Student Data Privacy course for relicensure and require all school employees to have data confidentiality training; Utah Student Data Privacy Teacher Relicensure Course, Canvas (last visited Sep. 7, 2018) https://usbe.instructure.com/enroll/JN3LRG; FERPA Basics Introduction, Utah State Board of Education, YouTube (Jul 17, 2018) https://www.youtube.com/watch?v=0M7juYs8Yh4&list=PLh6c2lcPJFukLSb4eN5veXsCRiloVvfte.
18. Educators Guide to Student Privacy, Future of Privacy Forum & ConnectSafely (last visit Sep. 7, 2018) https://ferpasherpa.org/educators/.
19. Student Privacy 101, Department of Education, https://studentprivacy.ed.gov/; Student Data Privacy Consortium, https://secure2.cpsd.us/a4l/; Coalition for School Networking, https://cosn.org/ProtectingPrivacy.