Policy recommendations for tech use in remote learning: Protecting students' privacy and access to education

November 2020

Access Living
ACLU of Illinois
Brighton Park Neighborhood Council
Chicago Lawyers' Committee for Civil Rights
Children's Screen Time Action Network
Civitas ChildLaw Center
Hartlieb & Horste, LLC
Illinois Families for Public Schools
Parent Coalition for Student Privacy
Raise Your Hand for Illinois Public Education

The use of technology in K-12 public schools has vastly expanded in the switch to remote learning due to the COVID-19 pandemic. This expansion compounds existing concerns about the privacy and equity implications for the use of ed tech.

The pressure on schools to attempt to recreate in-person school virtually has heightened concerns around this issue. Remote-learning technology has not necessarily been rolled out with careful thought given to protecting students and their personal information nor to clarifying or revising existing privacy policies.

The need and desire of school staff to provide education and build community for students must be balanced with protections for these children's privacy and security.

We need to keep in mind that surveillance does not equal safety. Surveilling students via technological means may very well have the opposite effect, particularly for those who are already subject to disproportionate policing outside and inside schools: students of color, especially Black and Indigenous students; students with disabilities; undocumented students; and low-income and poor students. The risks presented by this surveillance, even if they do not materialize, can traumatize these students and their families.

The policy recommendations here are meant to take all of the above into account.

Camera-on policies

Students should not be forced to turn on their cameras during live video conference sessions for remote learning. Students and families may have a variety of reasons for not wishing to turn their cameras on, whether from the mental burden of seeing oneself on camera, the risk of revealing victimless, lawful or embarrassing activities in the home, or the discomfort with sharing their living environment with peers and teachers. The push to have synchronous video conference sessions mirror the school day in length makes the former worse. The latter is an equity issue because it is especially acute for families with undocumented household members, families who are living under orders of protection and families in temporary living situations.

Furthermore, streaming video from home means exposing yet another environment to surveillance and policing. This can lead to incidents like those in Colorado and Louisiana this fall where Black children were suspended because of school employees viewing objects (a toy gun and a BB gun, respectively) on camera, which were legally present in the home.

Finally, the inadequacy and inconsistency of internet access may impede the use of video, and camera-on requirements compound this existing inequity. Use of virtual backgrounds also depend on computer capabilities and the physical environments and are unlikely to be a remedy for many families.

Teachers must be informed that asking students to share video or photos of themselves online has implications for both privacy and equity. Live instruction time should provide students with a variety of modes to participate and demonstrate their engagement and learning, including oral or typed discussion, use of polls, virtual raise hands/thumbs up, etc. Punitive consequences, like lowering grades or recording students as absent, should not be assigned to compel students to keep cameras on. Schools should be wary of overreach that potentially violates 4th Amendment protection against unreasonable searches and seizures in a family's home. Schools should also not use cameras to enforce dress codes that have little relevance to the virtual educational environment and that unfairly target students—particularly Black female students, who are disproportionately likely to experience punitive dress code enforcement.

To this end, schools should provide clarity on and revise their codes of conduct and behavior; some policies should not be applied in a home environment. For example, many objects and behavior not permitted on school grounds are legal in other environments, and, as such, may appear on camera. That said, school personnel are mandated reporters in most states, and so must report instances of suspected child abuse or neglect.

Written consent should be obtained from parents explaining the risks and benefits of live video streaming during synchronous learning. And, regardless of whether parents have consented to video streaming, students should always be permitted to participate in class without turning on video. See item (9) in this parent letter from Cambridge (MA) Public Schools for model language for a camera-opt-in policy.

Recording video conference sessions

Video recording should be limited to employees for the purpose of providing asynchronous instructional materials given the constraints of the pandemic. If students are to be recorded, teachers should not record students without clear notification of and consent from parents, for students under 18, and from students themselves over 18. Recording should never be obligatory for students, including for one-on-one sessions of a sensitive nature, e.g. counseling and therapy. Families must receive clear information about their rights to inspect, correct, receive copies of and, for children 13 and under, delete recordings. Consent should be entirely separate from general media consent forms distributed at the start of the school year.

Montgomery County (MD) Public Schools' detailed explanation of the use of video recording for parents is a good example of a policy clearly laying out when and how recording will take place; how long recordings will be available and to whom; and parents' right to opt out of having their children recorded. In addition, see the Clark County (NV) School District's guidance for administrators (pp. 9-10 and 90-91) for model language for employee guidance on recording video conference sessions.

Observers in the virtual classroom

Schools/districts should issue clear guidelines to allow parents, guardians or other participants, for example childcare workers or family members, to assist their child in participating and/or to observe live video-conference sessions. This is especially important for students with disabilities and/or young students who need assistance to participate in video conference sessions. It is also important for students who may not have a location at home that is not shared with others during school hours. Failing to address this issue disproportionately impacts Black and Brown students who are more likely to be homeless, "doubled up" or in temporary or overcrowded households during the pandemic. Guidelines or policies developed for in-person learning should be updated and should be in accordance with the US Department of Education's guidance in spring and the Letter to Mamas issued prior to the pandemic.

Use of surveillance software to monitor devices

Many students are participating in remote learning with school-owned devices. Schools may be monitoring these devices remotely with software including GoGuardian, GSuites for Education, etc. Schools may also be monitoring the use of *non*-school owned devices. Monitoring the activities of students or their family members who are not on school grounds and not participating in online instruction impinges on the civil rights of students and families. Devices, whether school-owned *or* family-owned, should *only* be monitored *during* synchronous learning for strictly delimited instructional purposes, e.g. assisting students with technology use remotely. The parameters of any monitoring should be made clear to students and their families, and those parents whose children need such assistance should be provided with the opportunity to opt-in to monitoring via written informed consent.

Students and families should be informed of the role of any browser in monitoring online activity and physical location, especially for the use of non-school owned devices. No third party provider of a computer hardware or software should be able to collect, use, generate or retain student data without explicit parental "opt in" permission. No data should be collected during this time of remote learning, unless it is directly necessary to the educational purpose for which it is presently being used. See this report from the ACLU of Rhode Island for clear policy recommendations on restricting schools' access to student devices.

Finally, schools' acceptable use policies should not include blanket statements that students have no expectation of privacy when using school devices and networks. Students should never be forced to choose between maintaining their privacy and receiving an education. Especially during remote learning, data that is part of students' educational records as defined by federal, state and local privacy laws is stored and transferred on devices and networks. Students and families most certainly have an expectation that the data held on school-owned devices and networks is subject to the protections afforded by those laws.

Use of surveillance software for proctoring tests remotely

Proctoring software (e.g. ProctorU, Proctorio) presents many of the same issues as surveillance software, but it is more likely to include biometric information, like face recognition data, eye gaze tracking, keystroke patterns, and also surveillance of a child's physical

environment, not just their device, via engaging the camera and microphone.

Even before the pandemic, high-stakes standardized tests were problematic from an equity perspective and now are even more likely to exacerbate inequity for the most marginalized students. Attempting to administer high-stakes standardized testing to children away from the classroom is impractical, expensive, and, since testing conditions will not match those the test was designed for, results will not be valid or reliable. Indeed, remote test monitoring tools, which range from facial recognition technology to eye focus monitoring, have very high fail rates that result in students who did nothing wrong being accused of cheating. Rather than ratcheting up attempts to monitor test takers, schools and teachers should implement methods of assessment during remote learning that do not require surveillance software. Authentic assessment methods like portofolio-based and performance-based assessments do not require subjecting students to invasive technology in order to demonstrate evidence of learning.

Policy transparency for families

Schools should not only establish clear policies but also make information about these policies easy to access—online (including for mobile devices) and in hard copy for families with limited internet. These policies should be written at a 4th grade level reading standard and be translated for non-English speaking parents. Moreover, schools should also explicitly identify a point of contact and a set of procedures for parents and students to get complaints and/or concerns related to privacy, surveillance or data security heard and addressed. Ideally, schools should designate responsibility for this area to an existing school records officer or privacy officer. ■