Resources Memo: COVID-19

How can districts promote a safe and secure digital learning environment?

Regional Educational Laboratory West

From the National Center for Educational Evaluation at IES

How can districts promote a safe and secure digital learning environment?

Education leaders are quickly working to provide a safe and secure digital learning environment for students. But educators and families still have questions in three areas: securing the digital classroom, how to ensure students display good digital citizenship, and privacy and permissions.

What can districts and families do to make sure online learning is safe and secure?

With more teachers and students engaging in remote learning, reports of breaches in security are increasing. Educators, students, and families can take actions to protect against "trolling" and other disruptions, ensuring their digital classrooms are secure.

Here are some things educators can do:

1. Know and use the protections built into digital classroom platforms.
2. Work with teachers to institute best practices around security such as making sure video conference links are not posted publicly, being aware of each child's media release status, and safely handling students' personally identifiable information (PII).
3. Explicitly teach students safe practices, such as <u>never</u> sharing their passwords or room links.

Related Links

- *EdTech* Magazine has a <u>2-minute video</u> sharing ways to maintain cybersecurity.
- The Wide Open School website from Common Sense Media has a page for <u>setting up the virtual classroom</u> with information specific to using Apple, Google, and Zoom.
- Zoom published an information sheet about <u>protections, privacy, and permissions</u> and EdSurge has more Zoom <u>safety and privacy tips</u>.
- Common Sense Media has curriculum for all grade levels in <u>privacy and security</u>. Some of their curriculum is available in Spanish as well as English. A free account is required to unlock the lessons.
- The ConnectSafely website offers a <u>parent guide to cybersecurity</u> and also has tips for home internet <u>safety and security</u>, from setting passwords to online safety FAQs. Some of the resources are <u>available in Spanish</u>.

> "Technological and student behavioral safety are the two things to work on. There are settings for the first but for the latter we need to think about how to use the technology to do the same things we do in the classrooms to provide structure, establish routines and expectations, and respectful norms of engagement."
>
> Joshua Harris
> EdTech Director
> Alisal Union School District
> Salinas, California

How can districts and families improve digital citizenship during remote learning?

Threats to student safety may also come from inside the virtual classroom. Helping students and families understand their roles and responsibilities for making the online learning environment a welcoming and safe space is critical. This is especially true for families that have internet access and technology devices for the first time. It is also important to support student social and emotional well-being and ability to cope with stress and anxiety.

Here are some things educators can do:

1. Establish and communicate norms for good behavior in digital learning environments to students and their families. Emphasize how classroom behavior expectations translate to a digital environment.
2. Explicitly teach grade-level appropriate digital citizenship to students.
3. Make a special effort to connect with and provide information to families who have technology in the home for the first time.
4. Support social-emotional learning to maintain relationships, foster resilience, and support emotional well-being.

Related Links

- Common Sense Media has digital citizenship lessons in English and Spanish.
- My Digital TAT2 has resource lists for educators and parents on digital citizenship and responsible internet use.
- Cyberbullying.org provides information, tips, and lessons for educators and families. Some are translated into Spanish.
- ConnectSafely has webpages related to cyberbullying for educators and families including topic-specific ones on LGBTQ cyberbullying and combating hate speech.
- CASEL supports social and emotional learning through a variety of tools, webinars, and other resources for educators and families.
- The *Social and Emotional Learning Toolkit* compiled by Common Sense Media provides information and a collection of resources.

How do we protect students' privacy when shifting to remote learning? Do we need special permissions from parents and guardians?

Schools and districts have always been obliged to protect students' personally identifiable information (PII) in the physical classroom. There are new considerations in the digital classroom. Also, nearly all districts have asked parents or guardians for permission for their students to engage in certain types of digital learning, usually in the physical classroom with teacher guidance. In moving to remote learning, these permissions may need to be revised.

Here are some things educators can do:

1. Review the privacy policy and terms of service especially for new technologies. Be sure teachers and administrators have information to protect students' privacy.
2. Provide families with information about what student PII can and cannot be collected and shared. Give simple, clear guidance on things they should watch for to protect their children.
3. Review and revise the parent and guardian permissions around technology use and digital learning as needed. Request parent or guardian consent.

Related Links

- The education page on the Future of Privacy Forum (FPF) website provides links to resources such as videos on student privacy, and a student privacy pledge in English and Spanish.
- ConnectSafely provides guides, blogs, and videos on tech safety for families.
- The FPF and ConnectSafely have created the *Educator's Guide to Student Data Privacy* and *A Parent's Guide to Student Privacy*.
- An FAQ on the Education Privacy Resource Center answers common questions.
- A group of national education agencies collaborated to produce *Ten Student Data Principles* and a resource center to learn more about protecting student data.