common sense®

Privacy and Distance Learning: Tips for Parents from Common Sense

With schools across the country moving to distance or hybrid learning during the pandemic, families are quickly figuring out how to navigate all the apps and websites kids are expected to use. From math games and e-readers to video-conferencing platforms and discussion tools, students and their families are juggling a lot of new technology right now.

Privacy and Distance Learning: Tips for Parents from Common Sense

Parents and caregivers may be wondering what risks these new tools pose and how they can minimize those risks. Which privacy settings should you use? Are parental controls available? To help families navigate these questions and more, Common Sense offers the following tips for keeping kids -- and their personal information -- safe during distance learning.

1. **Make privacy a family value.** Common Sense has a number of resources to help your family better understand **how to protect your privacy** and **why it's important**, including a **FAQ**, **advice articles**, and **classroom lessons on privacy and security**.

2. **Be careful what you share online about your kids and their classmates.** It's worth **knowing the facts** before posting pictures or letting **other people post pictures of your kids**. One important rule of thumb with distance learning: Don't post photos of your kid attending online class to your social media if their classmates are visible.

3. **Learn about parental controls to minimize distractions and data collection.** You don't need to be an expert at managing technology to help your kid stay safe and focused online. Check with your school's technology department to find out what safeguards and filters are already in place and what additional **parental controls** you can set up.

4. **Know whether classes may be recorded or monitored.** You should understand your school's policies regarding video-conferencing and classroom monitoring. It's useful to know how your kid's teacher will track student attendance or progress and what this means for their grades. And be sure that your kid -- no matter how old they are -- knows the **expectations for video-chatting in online classrooms**.

5. **Learn more about your school's educational apps and platforms.** Particularly now, schools have an important job in safeguarding student privacy. Parents and caregivers should **get familiar with their school's tools**, try to **learn about the risks** of the top distance learning apps, and **ask the school directly how they are protecting kids**.

6. **Ask questions, and exercise your privacy rights.** Remember that you have rights to access your kid's **education records** and any information that apps collect from your kid under federal and state laws.

For more resources on how to protect your kid's privacy during distance learning, visit www.commonsense.org.

With schools across the country moving to distance or hybrid learning during the pandemic, families are quickly figuring out how to navigate all the apps and websites kids are expected to use. From math games and e-readers to video-conferencing platforms and discussion tools, students and their families are juggling a lot of new technology right now.

Parents and caregivers may be wondering what risks these new tools pose and how they can minimize those risks. Which privacy settings should you use? Are parental controls available? To help families navigate these questions and more, Common Sense offers the following tips for keeping kids -- and their personal information -- safe during distance learning.

1. Make privacy a family value.

As your kid's school district embraces more online and digital learning tools, remember that your role as a parent and caregiver remains unchanged. You are still in charge of media and technology in your home, and you should still be setting expectations for your family. Because students must rely on technology daily for learning and communicating with friends, the first step is **using strict privacy settings in apps and on websites**. You can also go further by choosing **privacy-friendly web browsers**, limiting ad tracking on mobile phones and smart devices, and installing plug-ins like ad blockers and tracker blockers to limit how much data companies can collect about your kid while they're online.

It's important to have conversations with kids of all ages about how to keep their personal information safe online. **Common Sense Education's K–12 digital citizenship lessons on privacy and security** include family tips and conversation starters about privacy for families with kids in **grades K–5** and **grades 6–12**.

2. Be careful what you share online about your kids and their classmates.

It can be exciting to watch your kids attend class virtually via video. But parents and caregivers have an important responsibility to protect kids' privacy as well as the privacy of their classmates. Be choosy about what you share and with whom. The more you post, the bigger your digital footprint and the more data companies can collect. Be careful about sharing your child's full name, the name of their school, or their actual location online.

It's worth **knowing the facts** before posting pictures or letting **other people post pictures of your kids**. One important rule of thumb with distance learning: Don't post photos of your kid attending online class to your social media if their classmates are visible. Also, ask your kid before sharing their image on social media, and you may want to give your kid a veto over any sharing you do. It's always important to think about the effects sharing info about your kid can have on their **future well-being**.

You have a great influence on your kid. Monitor younger kids, and **help them understand** that what gets posted online can be difficult to remove or take back. **Talk to older kids about social media** and how they are portraying themselves to the world.

3. Learn about parental controls to minimize distractions and data collection.

Become familiar with the technology **your kid is using for school**. Some apps and most operating systems include **parental controls**. Parental controls can support you in your efforts to keep your kid's internet experiences safe, fun, and productive. They work best when used openly and honestly in partnership with your kids -- not as a stealth spying method. Make sure you explain why you're putting controls in place and how those controls will help keep them safe.

You don't need to be an expert at managing technology to help your kid stay safe and focused online. Check with your school's technology department to find out which safeguards and filters are already in place and which additional parental controls you can set up.

If your kids are distracted by non-school devices, these resources on smart speakers and video game consoles might be helpful:
Nintendo Switch parental controls *Xbox One parental controls* *PlayStation 4 parental controls* *Smart speakers and privacy*

4. Know whether classes may be recorded or monitored.

You should understand your school's policies regarding video-conferencing and classroom monitoring. It's useful to know how your kid's teacher will track student attendance or progress and what this means for their grades. Also, sometimes what a teacher can see or view on the platform is different from what students see, so it benefits everyone to have a discussion.

When students are using a video-conferencing platform, kids and their families should be mindful of what's in the background for both video and audio. Family members should try not to be in view of the camera or have conversations that can be picked up by the microphone. Some schools don't like virtual backgrounds because they're distracting or hog bandwidth. Ask if there are approved backgrounds, or see whether you can create your own by putting up a sheet or white poster board behind your kid's workspace.

The director of civil liberties and privacy at the U.S. National Security Agency **suggests** a series of policies schools should consider if classes are recorded:

- Recordings should be made available for a limited amount of time so students can review them if they miss class.
- Only families that have children in a class, rather than the entire school, can view any videos or recordings.
- One-on-one meetings with a child without a parent should be recorded, parents should be given an opportunity to review, and then the video should be deleted.
- Religious activities should not be recorded.
- Schools should provide clearly written notices that describe their recording practices.

These sorts of protections will be even more important as schools consider adopting tools that monitor students to ensure they aren't cheating. These services can collect a lot of student information -- from photos of kids' immediate surroundings and student images to remote monitoring of how students use their computers including typing behaviors. If your kid's school district is using a monitoring service, be sure to reach out to the technology team to ask what privacy and security protections have been put in place.

*Common Sense evaluated the privacy policies of several **distance learning services** like Zoom for Education, and our **Parents' Ultimate Guide to Zoom** is also a useful resource.*

5. Learn more about your schools' educational apps and platforms.

Particularly now, schools have an important job in safeguarding student privacy, and they should inform parents and caregivers how they're doing it. Schools should review and carefully curate which apps and services they use -- and which they expect their students to use -- to ensure both academic success and student data privacy and safety.

We know it isn't practical to read the privacy policy of **every app or tool your school wants to use**. Instead, ask school leaders how they vet and approve technology -- there should be a plan in place, rather than it being a free-for-all where individual teachers let students download anything. Check with your kid's school to get more information about which apps and websites have been school-approved. Parents and caregivers should ask the following questions, and your kid's school should have answers ready:

- **How does the school decide whether the educational software or apps it uses protect my kid's privacy?** Your kid's school should review the privacy policies of any software or device that requires your kid to log in with a screen name and password. **Common Sense's Privacy Program** is available to help parents and schools review educational apps with detailed privacy evaluations of popular products.

- **What information does the school collect, and how is it stored?** Schools need to be able to offer a clear educational purpose for collecting or using any personal information. Some schools are exploring new ways, such as thermal cameras and wearable technologies, to collect information about students that could be used to detect COVID-19. Schools should be very clear about what technology they are using for these purposes and what else they do with this information.

- **Who can get access to the school's list of students and their contact information?** **Federal law** limits who can get access to a school's directory of basic stuff like your kid's name, address, telephone number, and other general information. A school that's being careful will ask for consent before disclosing this or any other information. You should ask what your school does with "directory information."

- **When do I need to provide consent for my kid to use software at school?** Schools are allowed to provide consent on behalf of parents when they're using an app that collects information solely for educational purposes, such as an app that helps teachers take attendance. The school, the district, or an authorized teacher should ask parents to provide consent if any software or applications used in the classroom will collect information from students that's not for an exclusively educational purpose.

- **What sort of tracking does the school do on school-provided devices and software?** The school should have a written process about device searches (which includes notifying you before the device is searched). Schools should not install monitoring software, track the device's location, or remotely access the camera on a student's personal device. Be aware, though, that schools are required to monitor their internet networks under federal law, and some student data may be collected through that monitoring. Ask who within the school and district can access any device-specific tracking information and when this information is deleted.

You can read more about what answers you should expect from your school and why. Common Sense evaluated the privacy promises of the leading classroom management tools in use across school districts. Our Parents' Ultimate Guide to Google Classroom may also be a useful resource.

6. Ask questions and exercise your privacy rights.

Communication between parents and schools is more important now than ever. If something is confusing, just ask!

Remember that you have rights to access your kid's education records and the information that apps collect about your kids under federal and state laws. The **Family Educational Rights and Privacy Act** sets a **baseline of privacy protections** for educational records, while the **Children's Online Privacy Protection Act** protects information collected from children under the age of 13. (Take **our quiz** to see how much you know about children's privacy laws in the United States.) Many states have enacted laws that **further protect student's privacy**.

You can also bring complaints about how companies treat your kid's personal data and privacy to the **U.S. Federal Trade Commission** or your state's **attorney general**.

7. Don't panic!

While you may be feeling challenged by new digital learning tools and platforms from your school, the goals of teaching and learning haven't changed. Use your kid's teacher as a resource, and ask how you can best support your child. **Visit us online for more tips and helpful information.**