Supporting and Securing Students Online at Home

Grand Erie District School Board supports the Ministerial Order as an effort to contain the spread of COVID-19. The Board's Privacy Office created this fact sheet to support students and their families to assist them in transitioning to studying at home as part of the Ministry of Education's Learn at Home program. Technology offers many opportunities to keep connected and we are here to assist you in navigating risks, following best practices, and responding to your questions. Board policies and procedures, including those governing Privacy and Breaches, continue to apply. We are here to help you and the student(s) in your life make informed choices about privacy and information security at home.

What is the age to consent online?

Although Ontario's *Education Act* sets 18 years old as the age of consent for educational decisions, many apps/programs based out of the United States use 13 years old as the age of consent under the *Children's Online Privacy Protection Rule*.

I'm being asked to provide consent to a new app/program. Haven't I already consented to my student using technology?

Under the yearly Media Consent Agreement, parents/guardians who provide their consent are consenting to the sharing of student personal information. It is our responsibility to keep you informed about what applications are being used and how student information is shared so that you have an opportunity to ask questions or change your consent.

Making Informed Decisions

⇒ Work together to set house rules for using technology. Think about what devices can be used, for how long, and what apps or programs. The Office of the Privacy Commissioner of Canada has a do-it-yourself house rules for online privacy tool that may serve as a guide.

⇒ Make decisions together, whenever possible, so students feel greater accountability to the rules. Consider having older students sign this agreement. Ensure anyone supervising students online is aware of your house rules.

⇒ If you're not sure whether a program or app is appropriate for your student, you may find it helpful to consult Common Sense Media for reviews, privacy considerations, and other advice for adults.

⇒ Many apps and programs ask you to share personal information before you can access them. This may include your name, contact information, birthdate, household demographics, and sometimes banking, credit card, or other financial data. Some apps and programs also ask for access to your device's photos, videos, and the ability to record. Proceed with caution before providing any information or granting access to third parties.

⇒ Read privacy policies before clicking "yes." Remember, it is always your decision whether to consent to sharing information online!

⇒ Make decisions together about what to share on social media. Involve students in choosing pictures or videos to post, but respect their wishes if they do not want something shared. Adults may want to start conversations with older children and youth about topics such as privacy, online reputation, sexting and more with these guides from the Office of the Privacy Commissioner of Canada.

FAQs: Supporting and Securing Students Online at Home

Use these questions and ideas to spark discussions in your home about online privacy and responsible use of devices, apps, and programs.

What is your household's definition of privacy? Have a conversation with about what information should be private; what can be shared - by who, and how.

Not sure what apps your student(s) are using? Ask them to sit with you and show you what apps they use, how they use them, and whether personal information is shared.

Take an opportunity to lead by example. Take breaks, and set down devices when having face-to-face conversations. Involve students in decisions.

Technical — How can I minimize technical risks to student privacy and security?

⇒ Connect to a secure wireless network with a strong password. A secondary 'guest' network can be set up on most routers to limit bandwidth used by streaming services, games, and other apps.

⇒ Choose screen names and logins that minimize the chance of a student being identified online. Looking for some tips? Common Sense Media offers guidance on screen names and passwords for children and youth.

⇒ Update software when prompted - these updates often address security vulnerabilities!

⇒ Consider using settings and parental controls built into operating systems, devices, and apps, with things to consider, and step-by-step instructions available from Common Sense Media.

⇒ Set up separate accounts for each user on shared home computers, making sure students do not have 'administrator' privileges. Keep adults' business devices separate from ones used by students.

Supervision — How can I limit or monitor what my student is doing online?

⇒ Choose a central location for family computers where adults can supervise what students are doing online. A common charging station in the home can also serve as a 'parking lot' for devices when taking breaks from screen time, at meals, and overnight.

⇒ Consider using parental controls to limit internet connectivity to certain times of the day, but be mindful that online tracking and monitoring apps may produce overwhelming amounts of uninformative data so proceed with caution before exploring these.

Scams, Etc. — Are there increased risks of online malicious activity because of COVID-19?

⇒ Online scams always exist, but it's possible some are trying to take advantage of increased online activities. Looking for more information? Visit the Canadian Anti-Fraud Centre's COVID-19 Fraud Bulletin Alert.

⇒ Remember: if it sounds too good (or bad) to be true, it probably is! Scammers often offer rewards, convey a sense of urgency, or pretend to be someone you know to trick you into sharing information or downloading malware.

⇒ Both friends and strangers can pose risks online, so encourage your student to speak up if something makes them uncomfortable (i.e., cyberbullying, luring, inappropriate images or requests).

Questions? Contact foicoordinator@granderie.ca