The Schwarz Group, LLC

10 Tips for Enhancing Student Privacy During Remote (Virtual) Learning

1. For any app or program used for remote learning, consult the Privacy Policy to see what opt-out options are offered, and opt-out of all information collection and sharing permitted.
   - Even if the app, program or online site has taken the “Student Privacy Pledge,” parents should still read over the privacy policy themselves, as there is no active oversight or enforcement to ensure that the company is truly compliant with the promises made in the Pledge; the onus is on the parent.

2. Consider opting out of “Directory Information” sharing at the beginning of the school year. Directory Information includes your child’s name, date of birth, photograph and other personal information which could be shared widely in today’s Internet-connected world. While this won’t prevent Ed Tech companies from collecting data on your child’s use, opting out will prevent the school from sharing your child’s personal information with a host of other 3rd parties, such as the Military, SAT test prep companies, etc.

3. Make sure your child signs out of their school account(s) when engaged in non-school activities on the computer/device, so that actions while engaged in personal use are not inadvertently accessible to the school.

4. If using a personal device for school – whether it’s an iPad, iPhone, laptop or another device – go to “settings,” and turn off app permissions so that apps cannot access “location,” “contacts” or “photos”. If the app needs access to one of these services for school-related purposes, set the app to ask permission for access “each time” access is needed, so that you/your child remain in control and consciously chose when to allow access.
   - If your school uses a Google Chromebook or G-Suite for Education (Google), check your account settings to make sure that the YouTube Search/Watch History is turned off.
   - For more tips about Google Chromebook privacy settings read this (and other updated articles): https://www.techrepublic.com/article/pro-tip-how-to-configure-a-chromebook-for-ultimate-privacy/

5. Consider creating a throw-away email account with a free email service, without using your child’s real name or other personally identifying information, which can then be used for signing your child up for school-related apps or online accounts.
   - Relatedly, instruct your child that when s/he creates usernames and passwords for online accounts, s/he should **avoid** using personal identifying information, like name, date of birth, student number, pet name, school names, or other information that can easily be associated with, or linked to, your child.

6. Install a privacy-protective browser such as DuckDuckGo or the Brave browser on your child’s computer/device, and always use the settings to set the browser default to delete history upon closing of the browser.

7. To the extent your child uses a browser such as Safari, Chrome, Firefox, Microsoft Edge, etc., consider downloading and installing an ad-blocker like Privacy Badger or Ghostery. This not only blocks ads that may contain malware or other malicious code, but can potentially also prevent companies from tracking and profiling your child.

8. Have your child use different browsers for personal use and school/educational use, so that searches done on personal time are not available to, or accessible by, the browser used for school purposes.
   - Relatedly, have your child close all browsers (and browser tabs) before opening up a browser for school-related purposes, to minimize the bleed over of their personal browsing history.

9. When using Zoom or other video conferencing apps for online learning, be aware of your child's background, and remove any items that might reveal personal information about your child, such as a poster on the wall, family pictures, or other personal items. And consider asking the teacher if your child can leave the camera OFF (and covered) during the lesson, to protect their privacy; especially in Counties where live online lessons are recorded and retained for a period of time, parents should consider leaving the camera off to preserve privacy.
    - Consult counsel or file a complaint with the Education Department if a school mandates that the camera be kept on as a condition for participating in the live lesson, as there is no legal requirement to do so, and privacy is paramount; especially since the lesson is being given inside the student's own home.

10. To the extent possible, have your child use their computer/device in the living room or other public area of the house, so that you can maintain a watchful eye, and occasionally check in on their work.

Other Helpful Privacy-Related Pointers To Bear In Mind:

- Don't assume that the privacy policies of apps or online programs used by the school and/or assigned to your children (especially free ones) have been sufficiently vetted by their teachers or the school. Educational or classroom apps or online programs may not respect student privacy any more than other apps.
    - For example, Montgomery County Public Schools (MCPS) maintains a site dedicated to online apps and tools "vetted" for privacy and security. But when one looks at the criteria used by MCPS for privacy vetting, one learns that MCPS does not necessarily review the privacy policy and stay up to date on policy changes. So the responsibility falls back on the parent to review the privacy policy and ensure that they are comfortable with the privacy policy, and to take advantage of all opt-out opportunities, etc.

- When signing up for the SAT or ACT remember that providing answers to the questionnaires and surveys offered is ***optional***, and any information provided by your child in response to these questions will likely be disclosed and/or sold to 3rd parties. So fill in only required information. Opting out of the questionnaires, surveys and Student Search Services will not in any way affect your child's chances of getting into a college.

- Place a post-it note or other non-stick adhesive item (such as a Band-Aid) over the camera lens of your child's computer/device when the camera is not in use, to prevent inadvertent or malicious activation of the camera. Facebook founder Mark Zuckerberg and former FBI Director Comey both claim to do this for their children.

- Remind children under 13 years of age that pursuant to the *Children's Online Privacy Protection Act*, they **need your permission** before providing personal information to a website in order to open up a new account.

- Remember that under the *Family Educational Rights and Privacy Act* (FERPA), parents have a right to access and review their child's educational records as held by the school, as well as those records held by 3rd party Ed Tech providers used by the school for educational purposes (i.e., the apps, programs, online tools, and websites).
    - Relatedly at the end of each semester, or the school year, contact each online Ed Tech provider and request that they delete any records held by them on your child (depending on your school district, such requests may have to be funneled through the school, so check with your school for the proper process).

Additional Website Resources

http://https://www.studentprivacymatters.org
http://www.commercialfreechildhood.org

Contact: Joel.Schwarz@cyberprivacyconsultant.com **Website: http://cyberprivacyconsultant.com**