Some questions to help you quickly evaluate whether an app, website, product, or service will protect your students' information.🔍

Read full article here: https://www.connectsafely.org/eduprivacy/

1. Does the product collect Personally Identifiable Information?

FERPA, the federal privacy law applies to "education records" only, but many state laws cover ALL student personal information.

2. Does the vendor commit not to further share student information other than as needed to provide the educational product or service?

(Such as third party cloud storage, or a subcontractor the vendor works with under contract.) **The vendor should clearly promise never to sell data.**

3. Does the vendor create a profile of students, other than for the educational purposes specified?

Vendors are not allowed to create a student profile for any reason outside of the authorized educational purpose.

4. When you cancel the account or delete the app, will the vendor delete all the student data that has been provided or created?

5. Does the product show advertisements to student users?

Ads are allowed, but many states ban ads *targeted* based on data about students or *behavioral ads* that are based on tracking a student across the web.

TIP: Look for a triangle i symbol which is an industry label indicating that a site allows behaviorally targeted advertising. **These are never acceptable for school use.** This would be particularly important when evaluating non-education-specific sites or services.

6. Does the vendor allow parents to access data it holds about students or enable schools to access data so the school can provide the data to parents in compliance with FERPA?

7. Does the vendor promise that it provides appropriate security for the data it collects?

TIP: A particularly secure product will specify that it uses encryption when it stores or transmits student information. Encrypting the data adds a critical layer of protection for student information and indicates a higher level of security.

8. Does the vendor claim that it can change its privacy policy without notice *at any time*? This is a red flag—current FTC rules require that companies provide notice to users when their privacy policies change in a significant or "material" way, and get new consent for collection and use of their data.

9. Does the vendor say that if the company is sold, all bets are off? The policy should state that any sale or merger will require the new company to adhere to the same protections.

10. Do reviews or articles about the product or vendor raise any red flags that cause you concern?