

Evaluating Edtech Tools for Privacy Checklist

This information is shared with permission from the Student Privacy Compass as part of the Student Privacy Toolkit for School Districts.

School districts rely on hundreds of third party partners to enhance teaching and learning- this includes student information systems, progress monitoring tools and even educational apps. Administrators are tasked with putting a data governance program in place to vet all tools and ensure they uphold certain student privacy protections- this includes the edtech tools used in classrooms.

Before adding a new tool to the classroom, educators should know if that vendor creates a profile of students for non-educational purposes or if any advertisements are shown to students while using the product. The list of questions below can help educators in the vetting process.

- Does the app collect personally identifiable information (PII)?

| Yes | No |
|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> |

- What other types of data (de-identified data, aggregate data, metadata) are being collected?

- Does the vendor commit to not 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)?

| | |
|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> |
|--------------------------|--------------------------|

Tip: The vendor should clearly promise never to sell student data.

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

| | |
|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> |
|--------------------------|--------------------------|

Tip: When schools share student data under FERPA's "school official" exception, vendors are not allowed to create a student profile for any reason outside of the authorized educational purpose.

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

| | |
|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> |
|--------------------------|--------------------------|

Yes No

- Does the product show advertisements to student users? Yes No

Tip: Many states ban ads targeted based on data about students or behavioral ads that are based on tracking a student across the web. Look for a blue triangle i symbol, an industry label indicating that a site allows behaviorally targeted advertising. These are never acceptable for school use. This is particularly important when evaluating non-education-specific sites or services.

- 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? Yes No

Tip: This is one of the criteria the FTC lists as required for a school to be able to provide consent on behalf of a parent.

- Does the vendor promise that it provides appropriate security for the data it collects? Yes No

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

- Does the vendor claim that it can change its privacy policy without notice at any time? Yes No

Tip: 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 companies must obtain new consent from users for collection and use of their data.

- Does the vendor state that the school is responsible for complying with the Children's Online Privacy Protection Act (COPPA)? Yes No

Tip: the FTC prohibits vendors from pushing COPPA compliance onto schools.

- Does the vendor say that if the company is sold, the service to the school or district is terminated? Yes No

Tip: The policy or contract should state that any sale or merger will require the new company to adhere to the same protections.

- Does the vendor provide notice and indemnify the school or district to take responsibility in the event it or one of its subcontractors experiences a data breach? Yes No

Tip: Some states have laws that require schools to notify parents when student data is breached.

For more information and resources on student data privacy, contact us at security@more.net.