Building a Privacy and Security Technology Vetting Program

Assessing the privacy and security practices of third parties with which your school system might wish to share student personal information is a critical component to any student data privacy program. One simply cannot responsibly share student personal information with a third party without first confirming what personal information will be shared, how it will be used, how it may be further shared, how it will be protected, and more.

This resource provides an overview of how to develop a privacy and security vetting program for third parties that will have access to student personal data.

> **This resource also supports:**
> **Trusted Learning Environment (TLE) Business Practice 1:**
> The school system has implemented a process for vetting online services for data privacy and security.
>
> **Examples of Evidence for the TLE Application:**
> Process documentation explaining how third party online services (apps, websites, data management platforms, etc.) are reviewed for alignment with legal requirements and school system data privacy and security policies.

1. **Get Leadership Support.** Make the case to leadership about why the work is needed (for example, for legal compliance, risk reduction, cost savings, etc.). Ask for the support needed to make the program successful.

2. **Build the Cross-Functional Team.** Don't assess privacy and security practices of third parties that don't align with curricular goals, are cost-prohibitive, or are likely to be rejected by the district for other reasons. Build a cross-functional team to collaborate and build a review process that considers all angles.

3. **Get Smart**. Review district policies addressing district compliance with applicable privacy laws and consider how you might apply them when student personal information is shared with a third party.

4. **Know What You Need to Know.** Document the list of questions that you'll need to ask to help you understand if a third party is able to comply with your district's privacy and security expectations. See below for resources to help inform your list.

5. **Decide on the Answers.** What will make a third party's privacy and security practices acceptable to your district? Know the right answers before you ask and create a "go/no go" list of non-negotiables.

6. **Decide How You Will Do the Work**. At a minimum, review the applicable privacy policy and terms of use or service for each third party. Request any additional information needed for your review. If you can, consider a technical review of the product or service to help verify some of what you've read.

7. **Create an Agreement**. Once you have determined that a third party's privacy and security practices are acceptable, you'll need contractual provisions articulating your district's privacy and security requirements for each third party to sign. Develop this with your legal counsel if you have one.

8. **Socialize the Plan.** Explain the "what" and "why" of the technology vetting plan with employees before you get started. Enlist help from leadership in stressing the importance of (and requirements for) following the process.

9. **Communicate Findings.** Decide how you will let employees know if a product or service is approved for use, not approved, or approved only under certain conditions. Consider making this information available to parents and other caregivers to build more transparency about the technology program.

10. **Start Somewhere.** It might be helpful to launch the process with some commonly used and beloved products and services already assessed (and hopefully approved) to build the foundation for the library of approved tools to come.

Additional Resources from CoSN:
- Student Data Privacy Toolkit Part 1: Student Data Privacy Fundamentals
- Student Data Privacy Toolkit Part 2: Partnering with Service Providers
- Privacy Questions for Service Providers
- K-12CVAT

Additional Resources from the US Department of Education Privacy Technical Assistance Center:
- Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices
- Responsibilities of Third Party Service Providers Under FERPA