Building a Privacy and Security Technology Vetting Program

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.

Districts have legal and ethical obligations to protect student data privacy throughout the data lifecycle. Given that, assessing the privacy and security practices of technology partners, service providers, and other third parties with which your district might wish to share student personal information is a critical component to any student data privacy program. Privacy and security diligence are needed prior to contracting.

Skipping this critical step leaves districts blind to the caliber of third party privacy and security practices, leaving the district open to legal, reputational, and other risks, particularly in the event of a data breach.

Further, one cannot comfortably know if a provider can live up to the terms of a data protection agreement if one hasn't done any privacy and security due diligence to verify the facts of the matter before engaging in the contract.

However, privacy and security are not the only criteria that need to be considered before engaging with a technology or other service provider that will have access to student personal information. Price, curriculum alignment, ease of implementation, required technical specifications, needed supports, and more all play a part in qualifying a product or service for entry into the district. Given that, a cross-functional team is typically needed to determine whether a particular product or service can be qualified for use in the district.

This resource is designed to provide an overview of how to develop the privacy and security portion of a vetting process for technology and other service providers that will have access to student personal data.

1. **Get Leadership Support.** If your district doesn't have a privacy and security vetting program in place, building and implementing such a program could represent a significant change in how district personnel operate. Don't go it alone. First, make the case to your Superintendent about why this is needed. There are many reasons why that should resonate. By way of example, assessing privacy and security practices of third parties in order to qualify the third parties to move forward with contracting will help:
    - Support district compliance with applicable federal and state student data privacy laws;
    - Reduce security risks by ensuring that student personal data is only shared with third parties that have been able to demonstrate their ability to comply with district security requirements, and avoid tools with lax security practices from operating on the district's network;
    - Save money and manpower by ensuring that the district is only supporting tools and services that are safe, appropriate, and widely used by district personnel;
    - Build trust with parents and other community members who can be assured that

the district is taking reasonable steps to protect student data.

While you're meeting with leadership, be sure to ask for what you need. For example, you might need support building a cross-functional team to collaborate on the work, developing policies to ensure that privacy and security vetting is required, or enforcing such policies. Ask leadership to help you remove any barriers you might anticipate.

2. **Build the Cross-Functional Team.** Don't spend time assessing privacy and security practices of third parties when their products or services don't align with curricular goals, are cost-prohibitive, or are likely to be rejected by the district for other reasons. Bring people together from applicable teams and collaborate with them on building a review process that considers multiple needs – some before it gets to the point of the privacy and security review.

3. **Get Smart**. Identify the individual or individuals who will be involved in the work and refresh on the legal privacy requirements for student personal information. Include a review of district policies that explain expectations for district compliance with the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), other federal education laws that include privacy provisions, and if applicable, your state student data privacy law(s). Review these policies with consideration for how you might apply them when student personal information is shared with a third party provider.

4. **Know What You Need to Know.** With the laws and policies in hand, consider what it will take to know whether or not a particular third party is able to comply with your district's privacy and security expectations. Does the provider seems to understand the criteria it needs to meet to remain qualified by the district as a school official? Does it operate in a manner that would support the district's compliance with FERPA with respect to use of the product or services? Where applicable, does the provider articulate its obligations under the Children's Online Privacy Protection Act (COPPA) and provide the appropriate notices? Do the provider's privacy and security practices align with applicable requirements under your state's student data privacy law(s)/

   To make those determinations, you'll need answers to a variety of questions. These will include, but may not be limited to:

   - Under what legal construct will the district be able to share student personal information with the third party? Does the third party meet the district's criteria to qualify as a "school official" under FERPA? If not, is there another applicable exception to the written parental consent requirement in FERPA that is appropriate?
   - What student personal information must be shared for the services to operate? Does district policy prohibit any of those data elements from being shared, either due to the sensitivity of the data or other criteria?
   - Who will the student personal information be collected from? How will it be collected?
   - Are there opportunities to provide the third party with personal information that is not necessary to obtain the basic services, but can be provided, perhaps for

additional but optional features? If so, what are the benefits to sharing additional information and how can the district control whether or not optional information is shared?

- What will each element of personal information collected be used for? Do those purposes all align with your district's definition of a legitimate educational interest?
- What sub processors might the third parties share personal information with and why? How does the third party ensure that its sub processors comply with privacy and security requirements consistent with what the district intends to impose on the third party?
- Will there be any commercial uses of personal information? This might include but would not be limited to targeted advertising.
- Are there age limitations or restrictions that apply to the product or service? If so, do those comport with your district's intended use cases?
- What are the components of the third party's security program? Does their security program align with a nationally recognized, industry standard security framework that meaningfully meets thresholds of legally articulated "reasonable security" requirements?
- How long will the student personal information be retained?
- How is the district able to request access, correction, and deletion of student personal information for a particular student or student(s), or deletion of all of the student personal information in the third party's care?
- Does the third party articulate that it will not make material changes to its privacy policy without agreement, and will not unilaterally modify the contract?

These are just some of the questions that need to be answered as part of an assessment of privacy and security practices. Additional resources to inform the work are provided at the end of this document.

Take some time to consider the questions that you need answered and make your list.

5. **Decide on the Answers.** Now that you have your list of questions, what sorts of answers are you looking for? It's not enough for a third party to answer the questions. They need to be providing you with the *right* answers for *your* district. What makes a third party's privacy and security practices acceptable to you? What would disqualify a product or service from consideration? What is something that could be acceptable with additional contract provisions from the third party? At a minimum, create a "go/no go" list of non-negotiables. This list may evolve over time, but knowing what you want the answers to be is the crux of doing the work. If you can, consider reviewing your list of questions and your go/no go criteria with your legal counsel before finalizing.

6. **Decide How You Will Do the Work**. Now that you know what you're looking for, how will you get it? There are 2 primary approaches:

    a. Read the Provider's applicable privacy policy and terms of use or service to help you understand their privacy practices. Request additional information about their privacy practices and request security documentation from the provider as needed

to further inform the review.

b. If you'd like to go a level deeper, do the review noted above and conduct a technical review of the product or service to help you verify some of the stated privacy and security practices.

Choose the path that is most suited to your district's capabilities and needs.

7. **Come to an Agreement**. Remember that after the privacy and security practices have been assessed, if you have determined that they are acceptable, you won't be able to move forward with approval for the district to start using the product or service until your district has contractual provisions in place articulating your district's required privacy and security standards. This may be your contract or the provider's contract, but the data privacy and security language should articulate the expectations for collection, use, handling, protection, secure disposal, disposition of parent and student rights and more. Work with your legal counsel if you have one to create or review any such contractual language.

8. **Socialize the Plan.** Lay the groundwork for implementing the vetting process so employees aren't caught off-guard when it happens. In advance of implementation, spend some time explaining the "what" and "why" of the work for employees, and set their expectations for how long a review process might typically take – including that it might be a bit bumpy at the start as everyone gets used to the new way of operating. Keep your door open for constructive feedback to help make things run more smoothly.

   This is also where your early work with leadership should start paying off. Enlist their help in stressing the importance of (and requirements for) following the process you've developed. This should be easy for your superintendent to do. After all, you're simply asking for their leadership.

9. **Communicate Findings.** Before you start: decide how you will let employees know whether or not a particular product or service is approved from a privacy and security perspective, not approved, or approved only under certain conditions. For example, perhaps a particular product or service might be approved but only if used with students above a certain age, or only with certain features turned off. Determine where you will store this information and how it will be made available to those employees who need it. Also consider making this information available to parents and other caregivers to build more transparency about the tools being used by the district to support their children's education.

10. **Start Somewhere.** Will you remove all products from your network and start fresh, start the process with any new products or services and try to backtrack over existing tools at a later date, or something in between? 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. Whichever path you choose, consider how you plan to get things started and be sure to communicate that with all impacted employees.

Additional resources:

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

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
- The Family Educational Rights and Privacy Act Guidance on Sharing Information With Community-Based Organizations