Suggested Contract Terms

After your School System chooses an online service provider, it is important to draft a contract that specifies how the provider will comply with your School System's security requirements. Drafting a contract should be done under the guidance of your School System's legal counsel; however, the following suggested contractual terms identify key components to consider including.

The contract should specify the services to be provided and the provider's obligations, including the following:

1. **Contract Scope**. Identify all elements that comprise the agreement and what order of precedence is followed in the event of a contradiction in terms. Identify any contract terms that are incorporated by reference (e.g. URL).

2. **Purpose.** If you have determined that the provider qualifies as a "school official" under FERPA and you will use the school officials exception as the vehicle for disclosing FERPA protected information to a provider, specify: (i) that the provider is considered a school official, (ii) the legitimate educational interest that the provider is fulfilling, (iii) the nature of the data collected, and (iv) the purpose for which any FERPA protected information is being disclosed.

3. **Data Collection, Use and Transmission.** Specify how the provider may use or collect data from the School System and your students, and any restrictions that may apply to the provider's use of that data and ensure that you bind the provider to those uses and restrictions. At a minimum, you should address the following:
   - Specify that the provider should only be permitted to use any information stored, processed, or collected as necessary to perform the services for the School System. Include a specific restriction on the use of student information by the provider for advertising or marketing purposes, or the sale or disclosure of student information by providers.
   - Specify any metadata the provider will collect (e.g. logs, cookies, web beacons, etc.).
   - Specify any data and metadata any 3rd party will collect (e.g. analytics, etc.) as a function of the use of the provider's service.
   - Specify that the provider should be restricted from accessing, collecting, storing, processing or using any school records, and student or parent information, for any reason other than as necessary to provide the contracted services to your School.
   - Specify when and how the provider may disclose information it maintains to other third parties. Under FERPA, providers may not disclose education records provided by your School System to third parties unless specified in your contract.
   - Specify whether the School System and/or parents (or eligible students) will be permitted to access the data (and if so, which data) and explain the process for obtaining access. Consider if the contract needs to specify whose responsibility it is (the provider or the School System) to obtain parental consent and facilitate parent's request to access student educational records.

- Specify that data collected belongs to the School System (and/or its users) and that the provider acquires no rights or licenses to use the data for purposes other than for the delivery of the service.
- Specify that a provider must disclose if it will de-identify any of the FERPA protected data that it will have access to and if so, require that the provider supply details of its de-identification process. When appropriate, you may want to retain rights to approve such a process prior to the provider using or sharing de-identified data in ways that are beyond the purpose for which any FERPA protected information is disclosed.

4. **Data Security.** Specify any security requirements that the provider must follow to the extent that it maintains, processes, or stores any information on behalf of the School System. At a minimum, the contract should address the following:
   - The provider must securely maintain all records or data either received from the School System or collected directly from the school, teachers, students, or parents in accordance with the security standards designated by the School.
   - Information, content and other data collected and stored from and on behalf of the School System and the students should be stored and maintained separately from the information of any other customer, school, or user.
   - The provider should restrict access to your School System's information to only those individuals that need to access the data in order for the provider to perform the agreed-upon services.
   - The agreement should identify what happens if the provider has a data breach. The agreement should identify the provider's responsibilities including the School System's point of contact, required notification time, and any obligations for end user notification and mitigation.
   - You should have the right to audit the security and privacy of your School System's or students' records or data.
   - Require the provider to notify you in writing about any changes that will affect the availability, security, storage, usage or disposal of any information.

5. **Data Retention and Disposal.** Assure the proper management and disposal of data or information pertaining to the School or its students. All data disclosed to the provider, or collected by the provider, must be disposed of by secure means to ensure that it is protected from unauthorized access or use.

6. **Bankruptcy or Acquisition.** Specify what happens to the data if the provider goes out of business or is acquired by another firm. Is there a source code or data escrow provision?

7. **Service Levels and Support**.
   - Specify the service levels the provider must meet and any credits you receive for any failure by the provider to meet these service levels.
   - Require the provider to supply the School with all the technical assistance you may need to use the services.

8. **Governing law and jurisdiction.** Typically a provider's default contract will specify that it is governed by the law of the provider's home state. Public institutions generally have significant restrictions on their ability to consent to such provisions under the School System's local state laws.
   - Check with your legal counsel about what law can govern contracts entered into by your School in light of your School's state laws.

9. **Modification, Duration, and Termination Provisions.** Establish how long the agreement will be in force, what the procedures will be for modifying the terms of the agreement (mutual written consent to any changes is a best practice), and what both parties' responsibilities will be upon termination of the agreement, particularly regarding disposition of student information maintained by the provider. Upon termination of the contract, the provider should return all records or data and properly delete any copies still in its possession, including archives and/or backups.

10. **Liability**. The provider should be liable for the activities of its staff and subcontractors.
    - The provider should generally have an obligation to comply with all applicable laws, including privacy laws.
    - If the provider will be collecting data from children under the age of 13, the provider should comply with COPPA.
    - The provider should be liable for any breaches in security or unauthorized third party access arising out of the provider's breach of its contract obligations.
    - The provider should be liable to the School System for any claims or damages that arise as a result of the provider's failure to comply with its obligations as a Cloud Service Provider under COPPA, FERPA, or other applicable laws.
    - Limits of liability should be consistent with market-tested commercial practices and should appropriately allocate risk between the Vendor as a Cloud Service Provider and the Customer as the owner of its Data.
    - The School System may wish to identify through negotiation specific categories of direct damages that would be excluded from traditional definitions of consequential damages.

*Endorsed by **The Association of School Business Officials International**.*