# THIRD PARTY CONTRACTOR REVIEW PROCEDURES

## STUDENT DATA PROTECTION

To the extent that a third party contractor has access to "education records" it is deemed a "school official" as each of these terms are defined under Family Education Rights Act (FERPA). When negotiating a contract or evaluating provider's Terms of Service (TOS) agreement and the school/district would need to provide students' personally identifiable information to the provider there must be an agreement in place which explicitly describes how the provider may use and share student data; how the provider will secure the data; and how data or information received from the District will be returned or destroyed when information is no longer needed.

## Memorandum of Understanding

When a school or District department would like to use an third party contractor for the purpose of providing education services, where students' PII may be shared, the school/department shall fill out a District *Internal Request to Share Students' Personally Identifiable Information to a Third Party Contractor* describing the parties involved; the purpose of the education service; what student PII will be shared; and how student PII will be used. This Request shall be submitted to the student data manager for approval. Prior to the school or District sharing students' PII, the third-party contractor shall sign a *Memorandum of Understanding to Share Students' PII,* as approved by the student data manager.

## Terms of Service Agreement Review

Many providers of online educational services and mobile applications relay on a Terms of Service (TOS) agreement that requires a user to click to accept the agreement in order to access the service or application for the first time. Depending on the content, TOS agreements, commonly referred to as clickwrap agreements, may lead to violations of FERPA, PPRA, or other laws relating to student privacy.

When a school or District employee would like to use an online educational service or mobile application to provide education services that relays on a TOS, and the school or District would need to provide students' PII to the service or application, the following procedure shall be followed prior to sharing any student PII.

1. **READ THE TERMS OF SERVICE**
   By understanding commonly used provisions, District employees will be better able to decide whether to request approval for online educational services and mobile applications through the internal request procedure. Look for these types of provisions in the agreement.

### WHAT TO LOOK FOR

- **Definition of data** should include all personally identifiable information and other non-public information.
- **Use of de-identified data** much have all direct and indirect personal identifiers removed. Provider agrees to not attempt to re-identify de-identified data and not to transfer de-identified data to any party unless that party agrees not to attempt re-identification.
- **Marketing and advertising** statement that provider will not use any data to advertise or market to students or their parents; data may not be used for any purpose other than the specific purpose outlined in agreement.
- **Modification of terms of service** statement that provider will not change how data are collected, used or shared without advance notice and consent of the District.
- **Data collection** statement that provider will only collect data necessary to fulfill its duties as outlined in the agreement.

- **Data use** is only for the purpose of fulfilling its duties and providing services under the agreement.
- **Data mining** is prohibited for any purposes other than those agreed to by the parties. Prohibit mining of user content for purpose of advertising or marketing to students or their parents.
- **Data sharing** is prohibited without prior written consent.
- **Data transfer or destruction** must ensure that all data in providers possession will be destroyed or transferred to the school/district when the data are no longer needed for their specified purpose.
- **Rights and license in and to data** statement that gives school/district ownership of data to which the provider may have access. Does not give provider any rights to sell or trade data.
- **Access** to any data held by provider shall be made available to the school/district upon request.
- **Security controls** statement that provider shall store and process data in accordance with industry best practices and notify school/district in the event of a security or privacy incident.

2. **PRINT AGREEMENT**
   If the agreement generally complies with these provisions, print the agreement and proceed to step 3. If the agreement does not provide the appropriate protections, look for another service or application that will provide the necessary protection of students' PII.
3. **COMPLETE REQEUST FORM**
   Complete an Internal Request TOS Agreement form including the principal's/director's signature.
4. **SUBMIT**
   Submit the TSO agreement and completed Internal Request TOS Agreement form to the student data manager.
5. **AWAIT APPROVAL**
   When approval is given by the student data manager to use the service/application, the school/District may share necessary student PII to the contractor.

For additional guidance on what to look for in a TOS agreement, see the Privacy Technical Assistance Center's Privacy-Related Terms of Service Provisions.

**STUDENT DATA MANAGER:**
Bryce Barth
Assessment Department
(801) 402-5229
bbarth@dsdmail.net

## Privacy-Related Terms of Service Provisions

The "GOOD!" column contains best practice recommendations for TOS privacy provisions. If you see this language in your TOS, it is a positive indication that the provider is making a good faith effort to respect privacy. The "WARNING!" column contains provisions that represent poor privacy policy and may violate FERPA or other statutes. Given that few TOS agreements will be worded exactly like the "GOOD!" or the "WARNING!" column, the final "EXPLANATION" column provides context to help you interpret the rationale behind the provisions.

| | | | | Source: Privacy Technical Assistance Center |
|---|---|---|---|---|
| | **Provision** | **GOOD!<br>This is a Best Practice** | **WARNING! Provisions that Cannot or Should Not Be Included in TOS** | **Explanation** |
| 1 | Definition of "DATA" | "Data include all Personally Identifiable Information (PPI) and other non-public information. Data include, but are not limited to, student data, metadata, and user content." | ***Beware of provisions that limit the definition of protected data:***<br>"Data only include user information knowingly provided in the course of using (this service)." | The definition of data should include a broad range of information to which providers may have access in order to ensure as much information as possible is protected in the agreement. Beware of provisions that narrowly define the "Data," "Student Information," or Personally Identifiable Information" that will be protected. |
| 2 | Data De-Identification | "Provider may use de-identified Data for product development, research, or other purposes. De-identified Data will have all direct and indirect personal identifiers removed. This includes, but is not limited to, name, ID numbers, date of birth, demographic information, location information, and school ID. Furthermore, Provider agrees not to attempt to re-identify de-identified Data and not to transfer de-identified Data to any party unless that party agrees not to attempt re-identification." | ***Beware of provisions that define de-identification narrowly (as only the removal of direct identifiers, such as names and ID numbers) or lack a commitment from Providers to not re-identify the Data:***<br>"Provider may use de-identified Data for product development, research, or other purposes, De-identified Data will have all names and ID number removed. | There is nothing wrong with a provider using de-identified data for other purposes; privacy statutes, after all, govern PII, not de-identified data. But because it can be difficult to fully de-identify data, as a best practice, the agreement should prohibit re-identification and any future data transfers unless the transferee also agrees not to attempt re-identification.<br>It is also a best practice to be specific about the de-identification process. De-identification typically requires more than just removing any obvious individual identifiers, as other demographic or contextual information can often be used to re-identify specific individuals. Retaining location and school information can also greatly increase the risk of re-identification. |

| Source: Privacy Technical Assistance Center | | | | |
|---|---|---|---|---|
| | **Provision** | **GOOD!<br>This is a Best Practice** | **WARNING! Provisions that Cannot or Should Not Be Included in TOS** | **Explanation** |
| 3 | Marketing and Advertising | "Provider will not use any Data to advertise or market to students or their parents. Advertising or marketing may be directed to the [School/District] only if student information is properly de-identified."<br><br>OR<br><br>"Data may not be used for any purpose other than the specific purpose(s) outlined in this Agreement."<br>*(If this provision is present, check to make certain there is nothing else in the agreement that would allow marketing/advertising).* | "Provider may use Data to market or advertise to student or their parents." | The TOS should be clear that data and/or metadata may not be used to create user profiles for the purposes of targeting students or their parents for advertising and marketing, which could violate privacy laws. |
| 4 | Modification of Terms of Service | "Provider will not change how Data are collected, used, or shared under the terms of this Agreement in any way without advance notice to and consent from the [School/District]." | "Provider may modify the terms of this Agreement at any time without notice to or consent from the [School/District]<br><br>OR<br><br>"provider will only notify the [School/District] of material changes." | Schools/districts should maintain control of the data by preventing the provider from changing its TOS without the school's/district's consent.<br><br>A provider that agrees to give notice of TOS changes is good; a provider that agrees not to change the TOS without consent is better. |
| 5 | Data Collection | "Provider will only collect Data necessary to fulfill its duties as outlined in this Agreement." | ***An absence of a data collection restriction (see left) could potentially allow vendors to collect a wide array of student information.***<br><br>***Also watch for:***<br><br>"If user gains access through a third-party website *(such as a social networking site)*. Personal information associated with that site may be collected." | If the agreement relates to FERPA-protected data, a provision like the one represented in the "GOOD!" column may be necessary. Including a provisions that limits data collection to only what is necessary to fulfill the agreement is a best practice.<br><br>Providers may view user access to their services through a third-party social networking site as an exception to established rules limiting data collection. |
| 6 | Data Use | "Provider will use Data only for the purpose of fulfilling its duties and providing services under this | ***Beware of provisions that contains the phrase:***<br><br>"without providing notice to users." | Schools/districts should restrict data use to only the purposes outlined in the agreement. This will help schools/districts |

| Source: Privacy Technical Assistance Center | | | | |
|---|---|---|---|---|
| | **Provision** | **GOOD!<br>This is a Best Practice** | **WARNING! Provisions that Cannot or Should Not Be Included in TOS** | **Explanation** |
| | | Agreement, and for improving services under this Agreement." | | maintain control over the use of FERPA-protected student information and ensure appropriate data use. |
| 7 | Data Mining | "Provider is prohibited from mining Data for any purposes other than those agreed to by the parties. Data mining or scanning of user content for the purpose of advertising or marketing to students or their parents is prohibited." | "Provider can mine or scan Data and user content for the purpose of advertising or marketing to students or their parents." | While data mining or scanning may sometimes be a necessary component of online services (e.g., for malware/spam detection or personalization tools), schools/districts should prohibit any mining or scanning for targeted advertising directed to students or their parents. Such provisions could lead to a violation of FERPA, PPRA, or State law. |
| 8 | Data Sharing | "Data cannot be shared with any additional parties without prior written consent of the User except as required by law."<br>OR<br>"The [School/District] understands that Provider will rely on one or more subcontractors to perform services under this Agreement. Provider agrees to share the names of these subcontractors with User upon request. All subcontracts and successor entities of Provider will be subject to the terms of this Agreement. | "Provider may share information with one or more subcontracts without notice to User."<br>OR<br>"Where feasible, Provider will require third-party vendors to comply with these Terms of Service." | While it is perfectly acceptable for providers to use subcontractors, schools/districts should be made aware of these arrangements and subcontractors should be bound by the imitations in the TOS. |
| 9 | Data Transfer or Destruction | "Provider will ensure that all Data in its possession and in the possession of any subcontractors, or agents to which the Provider may have transferred Data, re destroyed or transferred to the [School/District] under the direction of the [School/District] when the Data are no longer needed for their specified purpose, at the request of the [School/District]." | ***Beware of provisions that contains:***<br>"maintain(s) the right to use Data or user content." | While FERPA does not specify that education records shared under some of its exceptions must be returned or destroyed at the end of the contract, it is a best practice to require this. Data return or destruction helps limit the amount of personal information available to third parties and prevent improper disclosure. This provision also helps schools/districts maintain control over the appropriate use and |

| | | | | |
|---|---|---|---|---|
| | | | | **Source: Privacy Technical Assistance Center** |
| | **Provision** | **GOOD!<br>This is a Best Practice** | **WARNING! Provisions that Cannot or Should Not Be Included in TOS** | **Explanation** |
| | | | | maintenance of FERPA-protected student information. |
| 10 | Rights and License in and to Data | "Parties agree that all rights, including all intellectual property rights, shall remain the exclusive property of the [School/District], and Provider has a limited, nonexclusive license solely for the purpose of performing its obligations as outlined in the agreement. This Agreement does not give Provider any rights, implied or otherwise, to Data, content, or intellectual property, except as expressly stated in the Agreement. This includes the right to sell or trade Data." | "Providing Data or user content grants Provider an irrevocable right to license, distribute, transmit or publicly display Data or user content." | Maintaining ownership of data to which the provider may have access allows schools/districts to retain control over the use the maintenance of FERPA-protected student information. The "GOOD!" provision will also protect against a provider selling information. |
| 11 | Access | "Any Data held by Provider will be made available to the [School/District] upon request by the [School/District]." | ***Beware of provisions that would limit the school's or district's access to the Data held by Provider.*** | FERPA requires schools/districts to make education records accessible to parents. A good contract will acknowledge the need to share student information with the school upon request in order to satisfy FERPA's parental access requirements. As a best practice, parental access to their children's data should be seamless. |
| 12 | Security Controls | "Provider will store and process Data in accordance with industry best practices. This includes appropriate administrative, physical, and technical safeguards to secure Data from unauthorized access, disclosure, and use. Provider will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner. Provider will also have a written incident response plan to include promptly notification of the [School/District] in the event of a security or privacy incident, as well as best practices for responding to a breach of PII. Provider agrees to share its incident response plan upon request." | ***The lack of a security controls provision, or inclusion of a provision that sets a lower standard for Provider's security of Data, would be a bad practice and potentially violate FERPA.*** | Failure to provide adequate security to students' PII is not a best practice and could lead to a FERPA violation. |