Protecting Student Privacy While Using Online Educational Services: Model Terms of Service

About PTAC

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems and other uses of student data. PTAC provides timely information and updated guidance through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of student data systems. More PTAC information is available at http://ptac.ed.gov.

PTAC welcomes input on this document and suggestions for future technical assistance resources relating to student privacy. Comments and suggestions can be sent to PrivacyTA@ed.gov.

Purpose of this Guidance

In February 2014, PTAC issued guidance titled *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*. This *Model Terms of Service* document is intended to further assist schools and school districts in implementing that guidance.

In a traditional contracting process, the buyer and seller mutually agree on a set of terms and then sign a contract reflecting those terms. However, many providers of online educational services and mobile applications (i.e., vendors, contractors, and other service providers) instead rely 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. These types of agreements are commonly referred to as "Click-Wrap" agreements. Once a user at the school or district clicks "I agree," these terms will likely govern what information the provider may collect from or about students, what they can do with that information, and with whom they may share it. Depending on the content, Click-Wrap agreements may lead to violations of the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), or other laws, as well as privacy best practices.

PTAC offers this guidance to schools and districts to help them evaluate potential TOS agreements, and to offer direction regarding terminology frequently used in these agreements. By understanding commonly used provisions, schools and districts will be better able to decide whether to consent to a Click-Wrap or other TOS agreement for online educational services and mobile applications. The best practice recommendations below may also assist providers by suggesting approaches that better protect student privacy.

Schools and districts should exercise diligence when reviewing TOS agreements and follow established school and district policies for evaluating and approving online educational services and mobile applications. This will help ensure that the service or application is inventoried and evaluated, supports the school's and district's

broader mission and goals, and that the TOS is legally appropriate and compatible with the school's and district's policies and procedures.

Terms of Service and Privacy

When negotiating a contract or evaluating a provider's TOS agreement, remember your school's or district's obligations regarding student privacy. Make sure the agreement explicitly describes how the provider may use and share student data.

The table below summarizes PTAC recommendations regarding key TOS provisions. The "GOOD!" column contains our 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 lead to violations of FERPA or other statutes. While these provisions are based on terms that may actually be used in providers' TOS or privacy policies, they are presented here solely as illustrations of the types of provisions to look for while performing your own reviews of a provider's privacy TOS. Actual TOS may have strong privacy protections that differ from those detailed below. As 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.

Privacy-Related Terms of Service Provisions

	Provision	GOOD! 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 (PII) 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:* "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.

	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
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:* "Provider may use de-identified Data for product development, research, or other purposes. De-identified Data will have all names and ID numbers 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. 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.

	Provision	GOOD! 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." *Or* "Data may not be used for any purpose other than the specific purpose(s) outlined in this Agreement." (*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 students 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]." *Or* "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. 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.

	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
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.* *Also watch for:* "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 provision that limits data collection to only what is necessary to fulfill the agreement is a best practice. 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 Agreement, and for improving services under this Agreement."	*Beware of any provision that contains the phrase:* "without providing notice to users."	Schools/districts should restrict data use to only the purposes outlined in the agreement. This will help schools/districts 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 or the PPRA.

	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
8	Data Sharing	"Data cannot be shared with any additional parties without prior written consent of the User except as required by law." *Or* "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 subcontractors and successor entities of Provider will be subject to the terms of this Agreement."	"Provider may share information with one or more subcontractors without notice to User." *Or* "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 limitations 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, are 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 any provision that contains*: "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 maintenance of FERPA-protected student information.

	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
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 and 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 any provision 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.

	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
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 prompt 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.

Resources

Materials below include links to PTAC and other resources that provide additional best practice recommendations and guidance relating to TOS agreements. Please note that these resources do not necessarily address particular legal requirements (including FERPA requirements) that your school or district needs to meet when collecting, storing, disseminating, or releasing education records to a provider. It is always a best practice to consult legal counsel to determine applicable federal, state, tribal, and local requirements prior to entering into contractual agreements with providers.

Department of Education Resources

- Privacy Technical Assistance Center, U.S. Department of Education: http://ptac.ed.gov
- Privacy Technical Assistance Center, U.S. Department of Education, *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices* (2014): http://ptac.ed.gov/sites/default/files/Student Privacy and Online Educational Services %28February 2014%29.pdf
- Privacy Technical Assistance Center, U.S. Department of Education, *Written Agreement Checklist* (2012): http://ptac.ed.gov/sites/default/files/Written_Agreement_Checklist_0.pdf
- Family Policy Compliance Office, U.S. Department of Education: http://familypolicy.ed.gov

Other Government Resources

- FTC: Bureau of Consumer Protection Business Center, *Complying with COPPA: Frequently Asked Questions:* https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions
- National Institute of Standards and Technology, *Guidelines on Security and Privacy in Public Cloud Computing* (2011): http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf