CONNECTICUT STUDENT DATA PRIVACY PLEDGE

Connecticut General Statutes §§ 10-234aa through 10-234dd (the "Privacy Statutes") impose obligations on contractors who, in the course of providing services to public boards of education and public school students, gain possession of or access to student information, student records, or student-generated content (collectively, "student data").

By clicking "Agree" below, the contractor certifies and affirms that it will comply with all of the requirements of the Privacy Statutes, including the provisions of Conn. Gen. Stat. § 10-234bb regarding contracts with Connecticut public school boards of education (the "Boards").

Below is a summary of the Privacy Statutes, intended to provide contractors with notice of the Privacy Statutes' requirements. All contractors are advised to refer directly to the statutes themselves in determining whether they can sign this Pledge.

Definitions

For purposes of this Notice and Certification, the terms "contractor," "operator," "consultant," "directory information," "de-identified student information," "personally-identifiable information," "school purposes," "student information," "student records," "student-generated content," and "targeted advertising" shall be defined in accordance with Conn. Gen. Stat. § 10-234aa. "Education records" shall be defined by the Family Educational Rights and Privacy Act of 1974 ("FERPA"), codified at 20 U.S.C § 1232g (as amended) and its implementing regulations, 34 CFR 99.1 - 99.67 (as amended).

Contractual Provisions

Under Conn. Gen. Stat. §§ 10-234(a) and (f), effective July 1, 2018, all contractors must include certain contractual terms, described below, for all contracts with Boards through which the contractor gains possession of, or access to, student data. Any contract entered into between a Board and a contractor on or after July 1, 2018, that does not contain the required provisions is void.

Contracts must contain the following elements:

1. A statement that all student data provided or accessed pursuant to the contract is not the property of, or under the control of, the contractor.

2. The Board must have access to and the ability to delete any student data in the possession of the contractor. The parties must establish a means by which the Board may request the deletion of student data.

3. A statement that the contractor shall not use student data for any purposes other than those authorized pursuant to the contract.

4. A description of the procedures by which a student, parent or legal guardian of a student may review personally identifiable information contained in student data and correct any erroneous information, if any, in such student data.

5. A statement that the contractor shall take actions designed to ensure the security and confidentiality of student data.

6. A description of the procedures that the contractor will follow to notify the local or regional board of education, in accordance with Conn. Gen. Stat. § 10-234dd, when there has been an unauthorized release, disclosure or acquisition of student data.

7. A statement that student data shall not be retained by, or available to, the contractor upon completion of the contracted services unless a student, parent or legal guardian of a student chooses to establish or maintain an electronic account with the contractor for the purpose of storing student-generated content.

8. A statement that the contract and the Board shall each ensure their own compliance with the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g, as amended from time to time.

9. A statement that the laws of the State of Connecticut shall govern the rights and duties of the contractor and the Board.

10. A statement that if any provision of the contract or the application of the contract is held invalid by a court of competent jurisdiction, the invalidity does not affect other provisions or applications of the contract which can be given effect without the invalid provision or application.

Any provision of a contract entered into between a contractor and Board on or after July 1, 2018, that conflicts with any of the above provisions shall be void.

Ownership of Student-Generated Content

Under Conn. Gen. Stat. § 10-234bb(b), effective July 10, 2017, all student-generated content is the property of the student or the parent or legal guardian of the student.

Obligations Imposed on Contractors (Operators and Consultants)

General Obligations

Under Conn. Gen. Stat. § 10-234bb, effective July 10, 2017,

(a) All contractors must implement and maintain security procedures and practices designed to protect student data from unauthorized access, destruction, use, modification, or disclosure that, based on the sensitivity of the data and the risk from unauthorized access,

(1) use technologies and methodologies that are consistent with the guidance issued pursuant to section 13402(h)(2) of Public Law 111-5, as amended from time to time,

(2) maintain technical safeguards as they relate to the possession of student records in a manner consistent with 45 CFR § 164.312, as amended from time to time, and

(3) otherwise meet or exceed industry standards.

(b) A contractor may not use student data for any purposes other than those authorized pursuant to the contract or use personally identifiable information contained in student data to engage in targeted advertising.

Data Breaches

Under Conn. Gen. Stat. § 10-234dd(a), effective July 1, 2017,

(1) Upon the discovery of a breach of security that results in the unauthorized release, disclosure or acquisition of student information, excluding any directory information contained in such student information, a contractor shall notify, without unreasonable delay, but not more than thirty (30) days after such discovery, the Board of such breach of security. During such thirty-day period, the contractor may:

(A) conduct an investigation to determine the nature and scope of such unauthorized release, disclosure or acquisition, and the identity of the students whose student information is involved in such unauthorized release, disclosure or acquisition, or

(B) restore the reasonable integrity of the contractor's data system.

(2) Upon the discovery of a breach of security that results in the unauthorized release, disclosure or acquisition of directory information, student records, or student-generated content, a contractor shall notify, without unreasonable delay, but not more than sixty (60) days after such discovery, the Board of such breach of security. During such sixty-day period, the contractor may:

(A) conduct an investigation to determine the nature and scope of such unauthorized release, disclosure or acquisition, and the identity of the students whose directory information, student records or student-generated content is involved in such unauthorized release, disclosure or acquisition, or

(B) restore the reasonable integrity of the contractor's data system.

Obligations Imposed on Operators Only

General

Under Conn. Gen. Stat. § 10-234cc, effective October 1, 2016,

(a) All operators must

(1) implement and maintain security procedures and practices that meet or exceed industry standards and that are designed to protect student data from unauthorized access, destruction, use, modification, or disclosure, and

(2) delete any student data within a reasonable amount of time if a student, parent or legal guardian of a student or Board who has the right to control such student data requests the deletion of such student data.

(b) No operator may knowingly:

(1) Engage in

(A) targeted advertising on the operator's Web site, online service, or mobile application, or

(B) targeted advertising on any other Web site, online service, or mobile application, if such advertising is based on any student data or persistent unique identifiers that the operator has acquired because of the use of the operator's Web site, online service, or mobile application for school purposes.

(2) Collect, store, and use student data or persistent unique identifiers for purposes other than the furtherance of school purposes.

(3) Sell, rent or trade student data unless the sale is part of the purchase, merger or acquisition of an operator by a successor operator and the operator and successor operator continue to be subject to the provisions of this section regarding student information; or

(4) Disclose student data unless such disclosure is made:

(A) in furtherance of school purposes of the Web site, online service or mobile application, provided the recipient of the student information uses such student information to improve the operability and functionality of the Web site, online service or mobile application and complies with section (a), above

(B) to ensure compliance with federal or state law or regulations or pursuant to a court order,

(C) in response to a judicial order,

(D) to protect the safety or integrity of users or others, or the security of the Web site, online service or mobile application,

(E) to an entity hired by the operator to provide services for the operator's Web site, online service or mobile application, provided the operator contractually

(i) prohibits the entity from using student information, student records or student-generated content for any purpose other than providing the contracted service to, or on behalf of, the operator,

(ii) prohibits the entity from disclosing student information, student records or student-generated content provided by the operator to subsequent third parties, and

(iii) requires the entity to comply with subsection (a) of this section; or

(F) for a school purpose or other educational or employment purpose requested by a student or the parent or legal guardian of a student, provided such student information is not used or disclosed for any other purpose.

(c) An operator may use student information:

(1) to maintain, support, improve, evaluate or diagnose the operator's Internet Web site, online service or mobile application,

(2) for adaptive learning purposes or customized student learning,

(3) to provide recommendation engines to recommend content or services relating to school purposes or other educational or employment purposes, provided such recommendation is not determined in whole or in part by payment or other consideration from a third party, or

(4) to respond to a request for information or feedback from a student, provided such response is not determined in whole or in part by payment or other consideration from a third party.

(d) An operator may use de-identified student information or aggregated student information:

(1) to develop or improve the operator's Internet Web site, online service or mobile application, or other Internet Web sites, online services or mobile applications owned by the operator, or

(2) to demonstrate or market the effectiveness of the operator's Internet Web site, online service or mobile application.

(e) An operator may share aggregated student information or de-identified student information for the improvement and development of Web sites, online services or mobile applications designed for school purposes.

Data Breaches

Under Conn. Gen. Stat. § 10-234dd(b), effective July 1, 2017,

Upon the discovery of a breach of security that results in the unauthorized release, disclosure or acquisition of student information, student records or student-generated content, an operator that is in possession of or maintains student information, student records or student-generated content as a result of a student's use of such operator's Internet Web site, online service or mobile application, shall:

(1) notify, without unreasonable delay, but not more than thirty (30) days after such discovery, the student or the parents or guardians of such student of any breach of security that results in the unauthorized release, disclosure or acquisition of student information, excluding any directory information contained in such student information, of such student, and

(2) notify, without unreasonable delay, but not more than sixty (60) days after such discovery, the student or the parents or guardians of such student of any breach of security that results in the unauthorized release, disclosure or acquisition of directory information, student records or student-generated content of such student. During such thirty-day or sixty-day period, the operator may

(A) conduct an investigation to determine the nature and scope of such unauthorized release, disclosure or acquisition, and the identity of the students whose student information, student records or student-generated content are involved in such unauthorized release, disclosure or acquisition, or

(B) restore the reasonable integrity of the operator’s data system.