



## **BILLS AND POLICIES TO PROTECT STUDENT INFORMATION FROM USE BY PRIVATE EDUCATION TECHNOLOGY COMPANIES**

By: John Moran, Principal Analyst

### **ISSUE**

Provide a summary of the bills and policies introduced or adopted in Connecticut during the last three years to protect K-12 student personal information from private education technology companies.

### **SUMMARY**

There have been no bills introduced or enacted in the last three years for the purpose of protecting personal student information from private education technology companies. Existing federal and state law and state policy, which have been in place for years, provide certain safeguards for student personal information, but also include provisions that allow information to be shared under certain restrictions with private companies. There is also federal consumer law that protects the information of Internet users under age 13.

A state law passed in 2012 is not specific to education, but requires the state attorney general to be notified whenever a private company that holds personal information experiences an information security breach.

Because there are no recent bills or new policy specifically about student information, this report will (1) focus on a brief presentation of the existing law and policy and (2) include a summary of the state law regarding notification of security breaches.

### **BACKGROUND**

In Connecticut, as in all other states, student personal and academic information exists at two levels: the local school district and the state. Most of this information such as a student's name, age, performance on various tests, and other information

contained in students' transcripts originates at the local level and is then reported to the state. (For more information on what is reported to the state as part of the Public School Information System (PSIS) see OLR Report [2014-R-0220](#).)

At both the state and local levels there are agreements under which private education technology firms may have access to student information. At both levels, officials indicate that the agreements (1) restrict how the information can be used and (2) require security measures to protect confidential data.

OLR asked SDE for details and examples of the restrictive terms and security practices that it includes in such agreements. When the information becomes available, we will use it to update this report.

## **FEDERAL LAW**

There are two applicable federal laws.

### ***Family Educational Rights and Privacy Act (FERPA)***

The Family Educational Rights and Privacy Act (FERPA), enacted in 1974, protects the privacy of student educational records, with some exceptions ([20 U.S.C. § 1232g](#)). It requires schools, school districts, state education agencies, and federally funded institutions to keep confidential any personally identifiable information (PII) contained in a student's records unless (1) the parents (of students under age 18) or students age 18 or older ("eligible students") consent to disclose it or (2) one of the legal exceptions to the confidentiality requirement applies. One exception to the confidentiality requirement permits disclosure of information to organizations (public or private) conducting studies for, or on behalf of, educational agencies to develop, validate, or administer predictive tests; administer student aid programs; or improve instruction. An example in Connecticut of a private entity that has an agreement with the State Department of Education (SDE) that includes access to student information is Bloomboard, Inc., a teacher evaluation and support technology company. (For more on private consultants, including Bloomboard, under contract with SDE see OLR Report [2013-R-0356](#).)

In addition to the standing exceptions to confidentiality, the law permits local school districts to adopt a policy that designates certain student information as "directory information" that may be disclosed without prior consent. Districts must notify parents of this policy and allow them to restrict the type and amount of information included in the directory information for their child (for example, if the district's policy is to include the date of birth and email address, parents could request that information be excluded for their child). There is nothing prohibiting the disclosure of directory information to private entities.

## ***Children's Online Privacy Protection Act (COPPA)***

The federal Children's Online Privacy Protection Act (COPPA) regulates the online collection of personal information (name, address, etc.) from children under 13. It applies to commercial websites and online services directed at children and other commercial websites or online services that have actual knowledge that they are collecting information from children. Operators must post a link to their privacy policies on their homepages and on each page where they collect personal information from children. The act generally requires a parent's consent for a website to collect personal information from children. Exceptions include online activities such as contests, newsletters, and homework help (some of these require parental notification if there is continued contact between the child and the website). State attorneys general can sue in federal court to seek injunctions and obtain damages and other forms of relief for violations ([15 USC § 6501 et seq.](#)).

In 2012 the Federal Trade Commission (FTC), which enforces COPPA, announced it was adopting new regulations to strengthen and clarify enforcement of the law ([16 CFR § 312.1 et seq.](#)). Among other changes, the new regulations specify that photographs, videos, and geolocation information are included in the definition of personal information that cannot be collected without parental consent and notification.

The FTC has prepared a website on COPPA and children's online safety:  
<http://www.consumer.ftc.gov/topics/kids-online-safety>.

## **STATE LEVEL**

### ***PSIS***

SDE is charged in state law with (1) creating and maintaining the Public School Information System (PSIS) and (2) keeping confidential the student and teacher data included in the system. There are some exceptions to this confidentiality.

Local and regional boards of education are required to provide data on each K-12 student to SDE for inclusion in PSIS. This information includes:

1. state assigned student identification number,
2. student transcripts,
3. mastery test performance scores,
4. student attendance and family mobility, and
5. other data ([CGS § 10-10a\(b\)&\(c\)](#)).

One exception allowing disclosure requires SDE to provide information within 60 days on a written request by a full-time employee of an educational nonprofit organization recognized under the federal tax code ([CGS § 10-10a\(h\)](#)). The law makes the requesting party responsible for the reasonable costs of the request. It requires SDE to respond to these requests on a first-come, first-served basis.

### ***SDE and FERPA***

As does any state education department, SDE must abide by FERPA. SDE provided a Frequently Asked Questions (FAQs) document that outlines SDE's policy to protect confidential student information.

In the SDE's FAQs on information protections it notes:

On a limited basis, the SDE enters into agreements with organizations to perform audits and evaluations of federal- and state-funded programs, conduct research or administer and report on statewide assessments. Such agreements restrict terms of use and require stringent security practices to protect confidential data.

OLR has asked SDE for details and examples of the restrictive terms and security practices that it includes in such agreements. We will update this report when the information becomes available.

The FAQ document specifies that SDE retains ownership of all confidential data that it shares with any organization under an agreement.

### ***Information Security Breach Notification***

[PA 12-1, June 12 Special Session](#), § 130, requires any person conducting business in Connecticut who in the normal course of business owns, licenses, or maintains data that includes personal information to disclose any security breach to the attorney general without delay. By law, the person or business must also contact the state residents whose personal information has been, or is believed to have been, accessed by an unauthorized person. Failure to notify the affected residents or the attorney general is considered a violation of the Connecticut Unfair Trade Practices Act ([CGS § 42-110a et seq.](#)). This provision would apply to private education businesses who have or maintain student information.

## LOCAL LEVEL

Connecticut Association of Boards of Education (CABE) staff reports that they have developed model student information confidentiality policies for local and regional school boards to consider adopting. CABE believes that some districts have adopted the model policy, but staff does not know the exact number. (FERPA requires districts to adopt a policy.) The model policy states in part:

The district will only release records in accordance with the provisions of FERPA, as well as other relevant federal and state mandates as they relate to student records, personally identifiable information, and confidentiality.

The model policy goes on to note when personally identifiable information may be released without the permission of the student's parents (or the student if over 18). There are a number of situations under FERPA where this information can be released, including to organizations conducting studies for, or on behalf of, educational agencies such as school districts: (1) to develop, validate, or administer predictive tests; (2) administer student aid programs; or (3) improve instruction. It further states that (1) the release of this information must not permit personal identification of parents or students by anyone other than the representatives of the organization and (2) the information be destroyed after it is no longer needed for the study.

The model CABE policy, like FERPA, also allows the release of information in other situations that do not involve non-governmental entities, such as to comply with a judicial order or subpoena. (For more details on the types of situations under which FERPA allows information to be released without permission see OLR Report [2014-R-0127](#).)

JM:ro