Student Data Privacy

A Toolkit for Connecticut School Districts

Version 1.4
Monday, July 10, 2017

55 Farmington Avenue
Hartford, CT 06105
(860) 622-2224
www.ct.gov/CTEdTech

55 Farmington Avenue
Hartford, CT 06105
(860) 622-2224
www.ct.gov/ctedtech

Student Data Privacy

A Toolkit for Connecticut School Districts

Background

Members of the Data & Privacy Advisory Council of the Connecticut Commission for Educational Technology have assembled this list of research and resources to assist our state's K - 12 school districts in adopting best practices regarding the protection of student data accessible to third parties. This work stemmed from requests from school leaders for assistance in preparing for the rollout of Connecticut Public Act 189: An Act Concerning Student Data Privacy. We share these resources not as prescriptive, step-by-step measures but as useful guidance as districts look to review and modify their policies, practices, and communications regarding data privacy and security. District leaders should first consult their legal counsel to assess the specific measures they should take to comply with the law's new measures. Any advice or references from legal counsel in the references below come as informational only.

Understanding the Law

As a first step in assessing the implications of the law, district leaders should familiarize themselves with its content (https://www.cga.ct.gov/current/pub/chap_170.htm#sec_10-234aa):

- Definitions (Section 1)
- Operator Contract Terms (Section 2)
- Stipulations on Data Use (Section 3)
- District and Operator Notification Obligations (Section 4)
- Task Force (Section 5)

As of July 10, 2017, the provisions of HB 7207 are in effect, including these changes:

- Extends the date to July 1, 2018, by which local or regional boards of education must begin entering into written contracts with entities with which they share student data
- Modifies the deadline by which a board of education must electronically notify students and their parents or guardians about a breach of student data security from 48 hours to two business days after learning of the breach

55 Farmington Avenue
Hartford, CT 06105
(860) 622-2224
www.ct.gov/ctedtech

You may also find these secondary references of use:

- Alert from Shipman & Goodwin's School Law Practice Group
- Conference Call Briefing with Shipman & Goodwin, Hosted by Commission for Educational Technology, June 27, 2016 (MP3 Audio File)

District Resources

The following sections provide links and resources that districts should find useful in preparing for and maintaining compliance with the stipulations of PA 16-189.

Operator Contract Terms and Stipulations on Data Use

Districts will need to ensure that the privacy and security assurances outlined in the law apply to new or renewed agreements with operators entered into after October 1, 2016, when the law goes into effect. A full list of those assurances appears in Sections 2 and 3 of the statute. Closely following those requirements will help ensure compliance with the law. Please note that the statute articulates minimum requirements; districts may wish to negotiate terms that provide even stronger data protections than what the law demands. Other tools that districts can leverage as complements to Section 2 of the law include the following:

- Suggested Contract Terms: A thorough review by the Consortium of School Networking (CoSN) with Harvard Law School's Cyberlaw Clinic at the Berkman Center for Internet & Society. Includes the types of terms and assurances districts should pursue with educational technology (edtech) operators.
- Security Questions to Ask of An Online Service Provider: Also from CoSN, a checklist of questions to engage with edtech companies.
- Software Reviews
    - EdSurge Product Index: A general edtech software review portal, with some privacy and security information.
    - Education Framework: Fee-based toolset including EdPrivacy, with privacy quality scores of many edtech products, monitoring of changes to privacy policies, and district privacy quality reporting. The EdPrivacy product provides a parent dashboard of apps, Web sites, and contracts by student and teacher. Discounts apply to Connecticut schools.
    - Graphite Privacy Policy Browser: Useful privacy evaluations of a limited number of mobile educational apps, run by Common Sense Media.
    - LearnTrials: A freemium (basic features free, enhanced tools extra) provides crowd-sourced reviews of edtech products. While not focused on data privacy, the reviews can provide useful insights into potential software purchases.

District and Operator Notification Obligations

In addition to ensuring that contracts contain the data and privacy protections stipulated in the law, districts must adopt notification practices to communicate with students and families about the use of data in edtech products and any breach incidents.

District Adoption of EdTech Products

Within five (5) days of entering into any new or renewed contract with an edtech operator, districts need to communicate directly with students *and* their parents or guardians the following information (see Section 2(g)):

- Date of contract execution
- Brief description of the contract and the purpose of the contract
- The student information, student records, or student-generated content that may be collected as a result of the contract

Districts can create a standard template for these types of announcements to send via their emergency notification system or standard e-mail servers such as the following:

From: Stephanie Miller (smiller@anytown.k12.ct.us)
Subject: Contract Notice: Unicorn Data Systems
Good afternoon, On Friday, July 15, 2016, Anytown Public Schools entered into an agreement with Unicorn Data Systems (UDS) to provide reading intervention software to our school district. Use of UDS will enable Anytown to support students' literacy skills and equip teachers with data to support personalized instruction. You are receiving this notice because your son or daughter will be using the software in his or her classroom. The UDS platform captures and tracks the following information about your son or daughter: ● Name ● Grade ● Teacher ● School ● Current Reading Proficiency Level ● History of Completed Reading Assignments This data resides on secure servers maintained by the UDS team and is encrypted in transit using SSL technology as well as "at rest" on the UDS servers. Please be assured that Anytown treats the privacy of your student's data with the utmost seriousness and ensures compliance of all of our educational

55 Farmington Avenue
Hartford, CT 06105
(860) 622-2224
www.ct.gov/ctedtech

> technology partners with state and federal laws as well as general best practices. If you have any questions about the contract with UDS or the use of this software, please do not hesitate to contact me at smiller@anytown.k12.ct.us or (203) 456-7890.
>
> Regards,
>
> Stephanie Miller
> Privacy Officer and Director of Technology
> Anytown Public Schools
> (203) 456-7890 (O)
> smiller@anytown.k12.ct.us (E)
> 234 Main Street
> Anytown, CT 06999

Additionally, they must post this information to the district Web site.

Breach Notifications

Edtech operators must notify districts of data breaches resulting in the "unauthorized release, disclosure, or acquisition" (see Section 4) of student information within 30 days of discovering the incident and within 60 days of discovering a breach of directory information, student records, or student-generated content.

Districts have much more aggressive notification timelines, with an obligation to notify students and parents affected by any breach within 48 hours of learning about the incident. The law does not stipulate the content of district notifications in the case of a breach, but schools should attempt to share relevant information about the breach, as in the following example:

55 Farmington Avenue
Hartford, CT 06105
(860) 622-2224
www.ct.gov/ctedtech

From: Stephanie Miller (smiller@anytown.k12.ct.us)
Subject: Notice of Data Breach: Unicorn Data Systems

Good morning,

Despite Anytown's ongoing efforts to ensure the highest levels of data security and privacy in the use of educational systems, we regret to inform you information about your son or daughter may have been compromised in a recent breach of Unicorn Data Systems (UDS) reading intervention software. The UDS data is housed off site and includes the following elements:

- Name
- Grade
- Teacher
- School
- Current Reading Proficiency Level
- History of Completed Reading Assignments

UDS is actively investigating the causes and extent of the breach, and we will share updates with you as we receive them. Again, we regret that this incident has taken place and welcome any questions or concerns you may have.

Sincerely,

Privacy Officer and Director of Technology
Anytown Public Schools
(203) 456-7890 (O)
smiller@anytown.k12.ct.us (E)
234 Main Street
Anytown, CT 06999

In addition to e-mail sent to all affected students, parents, and guardians, the district must also post a notification to its Web site.

55 Farmington Avenue
Hartford, CT 06105
(860) 622-2224
www.ct.gov/ctedtech

Recommended Next Steps

The following recommended action items come from many of the above-referenced materials and general best practices:

- Legal Counsel: The recommendations in this toolkit and other sources cannot take the place of professional legal counsel familiar with interpreting current Connecticut and federal school laws. If your counsel has not yet engaged your district on these matters, do so before you experience a pressing issue.

- Privacy and Security Officers: Identify one or two leaders who will serve as point people for managing policy, security practices, incident response. Prepare a procedure to govern who is responsible for receiving notice of data breaches and how the district will respond to such notifications. When incidents take place, having these roles established will make for fast responses and clear communications with all stakeholders.

- Procurement Process: Districts should establish clear software procurement procedures, starting with teachers and administrators. The process should start by identify needs, articulating requirements, vetting potential existing solutions, reviewing software, negotiating terms, managing rollout and training, and accounting for support. Procuring software starts with learning objectives, not technology. Two excellent resources are the district-wide course from CoSN, Building Team Leadership for a Digital Transformation, as well as Shipman & Goodwin's Student Data Privacy Quick Reference Tool.

- Operator Data Security Protocols: While PA 16-189 provides specific contractual requirements, some of the statutory language merely points to steps that operators must take to ensure data security. Districts should consider developing a preferred description of the actions operators will take to ensure student record security and confidentiality, including administrative, physical and technical standards. As a departure point, see CoSN's Security Questions to Ask of an Online Service Provider.

- Software Inventory: Districts should develop a central list of software used and corresponding terms, data practices, contract dates, costs (even if free), etc. within its schools. Doing so will allow the efficient tracking of compliance, renewals, costs, changes to terms, etc. An easily searchable list can also help avoid duplicate purchases when similar needs arise and help identify opportunities for cost savings by combining separate license purchases. Districts can develop these in house or reference

55 Farmington Avenue
Hartford, CT 06105
(860) 622-2224
www.ct.gov/ctedtech

exemplars such as the inventory from Glastonbury Public Schools (MS Excel), graciously shared by Brian Czapla.

- Security Training and Best Practices: Regardless of changes to state and federal laws, school district leaders need to train employees on and support the continued use of security best practices, such as enforcing strong passwords, securing portable data drives, and ensuring a "need-to-know" policy of data access among staff. Districts should strive to make training personal, with broad-reaching benefits to all staff in and out of school to encourage engagement and adoption of best practices. Some useful resources include the following:

    - 2017 CEN Conference Session (Panel) ***(NEW)***
    - Common Sense Media Digital Literacy (Teachers and Students)
    - CoSN Trusted Learning Environment (TLE) Framework and Seal ***(NEW)***
    - Education Week Student Data Privacy Overview
    - iKeepSafe Privacy Courses for Educators and Families
    - KnowBe4 Training and Compliance Tools
    - Media Education for the 21st Century (MacArthur Foundation)
    - Multi-State Information Sharing & Analysis Center (MS-ISAC) ***(NEW)***
    - Privacy Technical Assistance Center (PTAC) Parent Training Videos
    - SANS Institute's Privacy and Security Training
    - StaySafeOnline.org (National Cyber Security Alliance) ***(NEW)***
    - Wisconsin State Department of Education Training Materials and Courses

- Community Engagement: Districts should take the lead on data privacy and security concerns, and they can also engage with parents and local subject-matter experts to inform and build consensus around policy and practice. Engaged parents can often prove the most supportive advocates of 21st-century, digital learning.

- Update District Web Site: As indicated above, districts must publish the list of software and apps in use as well as contract descriptions and dates. Any breach notifications will also need to appear on the district Web site. While the following examples do not meet all of these criteria, they provide good starting points (in alphabetical order):

    - Area Cooperative Educational Services (ACES) Data Privacy Page
    - Bethel (CT) Public Schools Privacy Information
    - Baltimore (MD) Digital Literacy and Privacy Site ***(NEW)***
    - Cambridge, MA: Balancing Classroom Innovation and Student Privacy

55 Farmington Avenue
Hartford, CT 06105
(860) 622-2224
www.ct.gov/ctedtech

- CoSN Student Data Policy Overview (Various Templates for District Use)
- Denver (CO) Public Schools Academic Technology Menu
- Somers (CT) Public Schools Privacy Information

- Student Records Policy: Review and consider revision to the board's Student Records Policy to ensure compliance with the PA 16-189 and relevant provisions of FERPA.

Further Reading and Reference

Terms of Service of Major Educational Technology Operators ***(NEW)***

In July 2016, district technology directors responded to a Commission survey to indicate the educational technology products whose terms were of greatest priority to bring under compliance with PA 189. The following list reflects the top systems ranked by priority by respondents. Linked text points to the data privacy policies as of this date. It does not begin to reflect the number of systems or apps that districts statewide are assessing but does offer a list of "crowdsourced" top priorities:

- PowerSchool
- Google Apps for Education
- IEP Direct (Frontline Suite)
- Naviance
- SNAP
- Destiny
- SchoolMessenger
- Discovery Education
- NWEA Assessments
- Renaissance STAR Assessments
- TurnItIn
- Schoology
- Edmodo

The Commission has partnered with the Department of Administrative Services (DAS) to negotiate data and privacy terms on behalf of Connecticut boards of education for educational software. Software that now complies with state statute appears on the following page:

http://www.ct.gov/ctedtech/cwp/view.asp?a=1182&q=253410

These titles will soon migrate to the Privacy Registry currently under development.

55 Farmington Avenue
Hartford, CT 06105
(860) 622-2224
www.ct.gov/ctedtech

Legal and Policy

The following excellent reference materials will provide greater depth and context for understanding the implications of Connecticut PA 16-189:

- CoSN Protecting Privacy in Connected Learning (CoSN - Registration Required)
- CoSN Privacy Toolkit (CoSN - Registration Required) ***(NEW)***
- Fordham Law National Study Finds Public School Use of Cloud Computing Services Causes Data Privacy Problems (Fordham Law School)
- Making Sense of Student Data Privacy (Bob Moore)
- Privacy and Student Data: An Overview of Federal Laws Impacting Student Information Collected Through Networked Technologies
- Privacy Technical Assistance Center (US Department of Education)
- Student Data Privacy Report (Education Week)
- Student Data Privacy: Moving from Fear to Responsible Use (Brookings Institute)

Acknowledgements

We greatly appreciate input from the following groups and individuals for their contributions to and review of this document:

Commission for Educational Technology Data & Privacy Advisory Council

- Jeffrey Kitching (Chair), Education Connection
- Brian Czapla, Glastonbury Public Schools
- Robert Jasek, Trinity College
- Brian Kelly, Quinnipiac University
- Scott Matchett, South Windsor Public Schools
- Stephen Nelson, Eastern Connecticut State University
- Jason Pufahl, University of Connecticut
- Bethany Silver, Bloomfield Public Schools
- Michael Swaine, Gaggle

55 Farmington Avenue
Hartford, CT 06105
(860) 622-2224
www.ct.gov/ctedtech

Shipman & Goodwin

- Benjamin FrazziniKendrick
- William Roberts
- Gwen Zittoun

Consortium for School Networking

International Society for Technology in Education

State Educational Technology Directors Association

Contact

If you have questions, comments, or suggestions for improvements to this document, please contact us.

Doug Casey
Executive Director
Connecticut Commission for Educational Technology
(860) 622-2224
doug.casey@ct.gov