CTEDTECH
Connecticut Commission for Educational Technology

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

Data and Privacy Advisory Council

Meeting Minutes

February 6, 2018

Attendees

- Ben FrazziniKendrick (Shipman & Goodwin)
- Bethany Silver (Bloomfield Public Schools)
- Brian Kelly (Quinnipiac University)
- Doug Casey (Commission for Educational Technology)
- Jason Pufahl (University of Connecticut)
- Michael Swaine (Gaggle)
- Scott Matchett (South Windsor Public Schools)

Agenda

1) Trusted Learning Environment (TLE) Program (Doug Casey)

2) Educational Software Hub (Doug Casey)

3) Student Data Privacy Updates

    a. Statute (Ben Frazzinikendrick)
    b. EU GDPR (Ben Frazzinikendrick)
    c. Task Force Timing (Doug Casey)

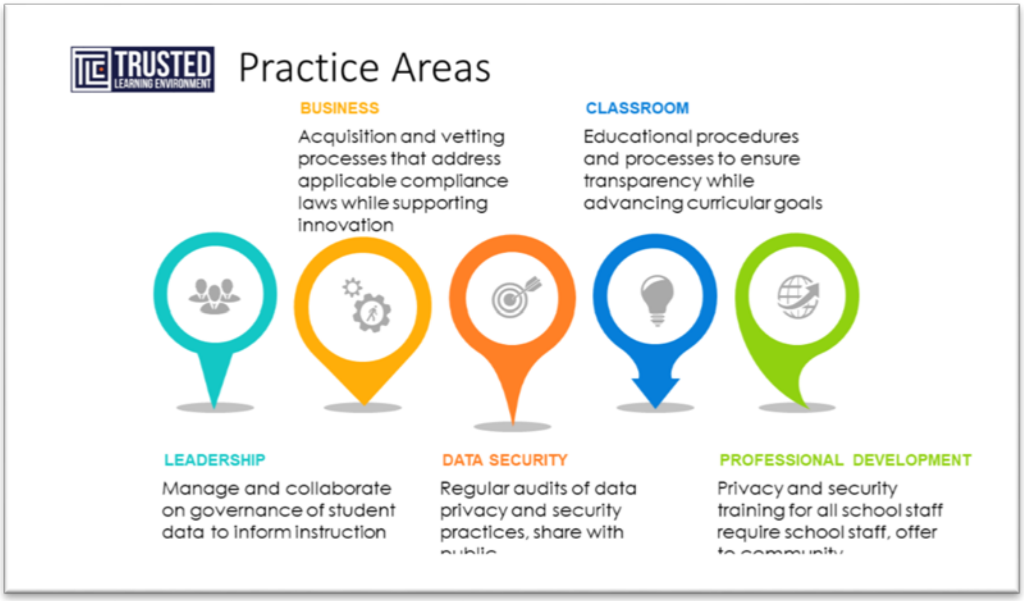
4) Collective Student Security Services (Michael Swaine)

Meeting Notes

The points below represent an assimilation of ideas rather than a verbatim or chronological record of points shared.

Trusted Learning Environment (TLE) Program

In an effort to support school district data and security best practices, the Data & Privacy Advisory Council has endorsed the Consortium for School Networking (CoSN) Trusted Learning Environment (TLE) framework, the first topic on the agenda. Doug Casey spoke to the framework, with five practice areas defined in the image below:



TRUSTED LEARNING ENVIRONMENT Practice Areas

BUSINESS
Acquisition and vetting processes that address applicable compliance laws while supporting innovation

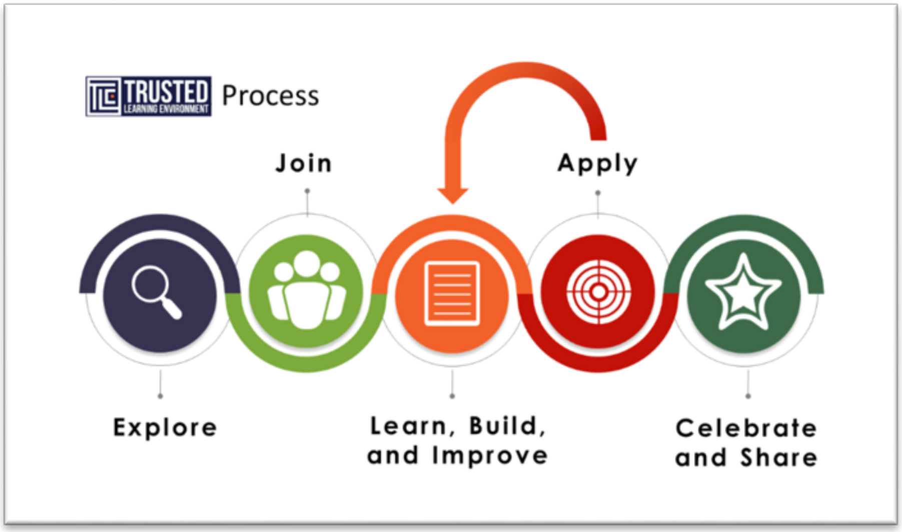
CLASSROOM
Educational procedures and processes to ensure transparency while advancing curricular goals

LEADERSHIP
Manage and collaborate on governance of student data to inform instruction

DATA SECURITY
Regular audits of data privacy and security practices, share with public

PROFESSIONAL DEVELOPMENT
Privacy and security training for all school staff require school staff, offer to community

The TLE framework provides districts with a set of evidence-based best practices upon which to build and improve upon a program to ensure privacy and security in school districts. The Connecticut CoSN chapter, CT Education Technology Leaders (CTETL), will host an orientation session [Thursday, February 22](), hosted by Linnette Attai, CoSN's TLE program lead. During that session, attendees will learn about the program and how to join the first statewide TLE cohort. Doug shared the process for districts to consider joining the cohort, conducting a self-assessment on data and privacy practices against the TLE framework, and undertaking efforts to obtain the TLE seal:



TRUSTED LEARNING ENVIRONMENT Process

Scott Matchett commented that security resources for districts remain important. Data privacy requires ensuring a secured environment, and security remains a difficult practice. For this reason, the TLE remains valuable to districts that work to earn the seal. At the very minimum, schools — especially smaller institutions or those with less mature practices — should use the TLE as a reference through which to assess their policies and procedures.

Brian Kelly asked about interest among Connecticut districts to join the cohort, with Doug offering that 35 districts had attended a similar orientation meeting in December. Districts will commit later this month to participate in the year-long program to develop and adopt policies and practices that they can use in applying for the TLE seal. Doug asked if a similar framework exists for higher education, with Brian and Jason Pufahl citing organizations such as Educause and the SANS Institute. However, colleges and universities do not have a standard, set framework such as the TLE for K – 12.

The group discussed the importance of students learning about and adopting "cyber hygiene," best practices in protecting their data and identity online. Brian Kelly noted that colleges provide the opportunity students, especially freshmen, to learn about security best practices and has spoken to students during Quinnipiac's orientation sessions, as well as other venues. Both he and Jason noted the top priority in higher education on protecting the intellectual property and other information assets of the institution and its staff, rather than on student data. Increasingly, college students use their own, personal accounts and accompanying data (e.g., Gmail and Google Drive documents), rather than students always leveraging school communications and data storage tools. Therefore, the onus of privacy and security continues to rest on individual students.

The group recognized the need to build cyber and digital literacy skills among K – 12 students and their families. Scott suggested having "Cliff Notes" versions of the Center for Internet Security (CIS) Controls, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and other free and low-cost resources. The group discussed the work of Scott Driscoll, founder of Internet Safety Concepts, who presents frequently on the topic of Internet safety to school communities. Data and Privacy Advisory Council members agreed to develop a list of resources for schools and perhaps a speakers' bureau. This work would also include conducting an informal survey of related resources that other organizations (e.g., parent teacher organizations, Girl Scouts and Boy Scouts, State agencies, etc.) have already developed.

Educational Software Hub
As a tool for assisting districts to comply with Connecticut's student privacy statute, the Commission launched the Educational Software Hub last fall. Doug provided updated usage data to the group:

- 98 Products Listed
- 1,402 Registered Users
- 105,000 Page Views in November

These numbers serve as encouragement that educational technology providers are visiting the state's site, http://StudentPrivacy.CT.gov, to learn more about the statute, sign the Student Data Privacy Pledge, and provide written assurances of compliance. As the group noted, however, the contractual components of the statute go into effect July 1 of this year, a hard deadline that educational technology companies and districts must meet in addressing the law's requirements regarding how these companies store, manage, and provide student and parent access to personal data and information.

Student Data Privacy Updates

Several members had suggested that the group address concerns around the Connecticut and other student data privacy laws as agenda items. The following sections contain synopses of these discussions.

Statute

Ben FrazziniKendrick noted the impending compliance deadline and expressed hope that districts and the companies they use to provide educational technology services and software would continue efforts to reach compliance with the state statute. This year is a short legislative session, designed to address budget issues only, making it unlikely that the law will change until next year's long session.

European Union General Data Protection Regulation

The group addressed the implications of the recent General Data Protection Regulation (GDPR) of the European Union (EU). This provision most likely impacts schools and colleges that have access to or store the data of students from the EU. The GDPR addresses the processing of personal data in the context of activities of a controller or processor in the EU, regardless of whether or not the data processing happens in the EU. A concern to educational technology companies in Connecticut and other U.S. states, the provisions also address the processing of personal data of individuals who are in the EU by a controller or processor (e.g., U.S. company) not in the EU.

The most obvious example of how the GDPR may impact districts and institutions of higher education comes in the form of exchange students or those from other countries enrolled in Connecticut colleges. Brian Kelly noted that the GDPR provisions have become the standard in some ways against which data protections take place at his institution, rather than singling out how Quinnipiac handles just the data of students from EU nations. The group would continue to monitor and share impacts of the GDPR requirements across institutions.

Task Force

The Connecticut acts that put in place student data privacy protections (PA 16-189 and PA 17-200) point to the creation of a Task Force that will "study issues relating to student data privacy." Appointees will define in more specific terms how students and parents can request access to their data, the form of notifications regarding data use and breaches, and other aspects of the statute. Doug shared that the Legislature is actively engaged in finalizing these appointments and convening the Task Force. He also shared some of the suggestions he has received regarding revisions to the statute, including better definitions of some terms (e.g., “de-identified information,” “ownership” of data, etc.); use of the Educational Software Hub’s Student Data Privacy Pledge as the basis of compliance; the exemption of what FERPA defines as “directory information”; and funding to support collective compliance efforts. When the Task Force convenes, the members will certainly have an opportunity to share the suggestions of their constituents to help make the law clear and sustainable while not sacrificing its sound protections of student data and information.

Collective Student Security Services

Michael Swaine opened a discussion around the need for greater assurances that school districts take measures to protect student safety online. Specifically, he called for revisions to the Children’s Internet Protection Act (CIPA). At the time of its writing, CIPA addressed protections by means of filtering, when the Web existed primarily as a means of information retrieval (i.e., one-way transmission). Times have changed, and technology has greatly increased in the capabilities it offers to students, teachers, and administrators. In the current era, Web-based, educational applications allow participants to create and share data across many different, collaborative platforms. Simply filtering content does not address threats to students.

Michael provided examples from the work of his own firm, Gaggle, in using both artificial intelligence and human monitoring to detect and provide notice to school administrators of incidence of online bullying and even plans to commit murder and suicide. His argument is that technology exists to extend protections of students, given the highly interactive nature of educational software.

The group heartily agreed with Michael’s suggestions, regardless of the educational software tools used for instructional or monitoring purposes. They discussed possible complementary efforts among groups such as Connecticut Appleseed as well as state and federal legislators. Members looked to share this idea within their professional networks and agreed that the best venue for addressing these concerns remains at the federal level, with possible revisions to CIPA and at least engaging Connecticut’s Senators and Representatives.

Doug thanked the group for their time and expertise and adjourned the meeting shortly before 4:00 PM.