Cypress-Fairbanks ISD
Trusted Learning Environment

Spring, 2018

Agenda

- Introductions
- Privacy and Security Concerns
- Legislative Focus
- Training Needs
- Support
- Trusted Learning Environment Seal
- National Focus
- District Focus

Privacy and Security Concerns

School System Leaders Are Concerned

- According to the results of the 2017 Consortium of School Networking (CoSN) Leadership Survey, **61%** of technology leaders identified privacy and security as a primary concern.

Parents Are Concerned

- In the 2016 Future of Privacy Forum survey results, **84%** of parents are concerned that their child's electronic education records could be hacked or stolen.

Incidents Are On the Rise By 100%

- Since 2016, hundreds of K–12 schools and districts experienced one or more publicly disclosed cyber incidents.

School District Must Take Action

- In 2016, an audit of some 1,200 web-based education software products by the nonprofit Common Sense Education found that nearly half the offerings didn't automatically encrypt student data.

Privacy and Security Concerns

- "If our student data is hacked, it might just be a test score, but it could also be their Social Security number, or their disability information," she said. "It can impact them for the rest of their lives."

Melissa Tebbenkamp,
Director of Instructional Technology,
Raytown School District

- "The first line of defense in protecting student privacy are our teachers, and we're not making sure that they have the tools to keep that data safe,"

Amelia Vance,
Policy Counsel
Future of Privacy Forum

Legislative Focus

- According to Data Quality Campaign, since 2013,
  - state legislatures have considered about 400 student data privacy bills
  - state legislatures have passed more than 70 into law
- Texas passed HB 2087, in effect September 1, 2017
  - Relating to restricting the use of covered information, including student personally identifiable information, by an operator of a website, online service, online application, or mobile application for a school purpose.

Data Privacy Training Needed

- Schools should target common missteps, such as recycling passwords or working with sensitive information on an unsecured Wi-Fi network.

- Ensure every teacher knows the basics of privacy laws, such as the Children's Online Privacy Protection Act, which requires parental consent for any web service collecting "personally identifiable information" of children under 13, including photographs and voice recordings.

- Train teachers to clearly inform parents about what student information their classroom technology will use and why.

Amelia Vance, Policy Counsel
Future of Privacy Forum

Districts should ask. . .

- "Before any bits get passed anywhere, educators should be trained to ask, 'Does this data need to be collected to help students learn?' If so, 'How is it going to be protected?' "

Bill Fitzgerald
Privacy Initiative Director
Common Sense Education

Student Data Privacy Consortium

- In the past four years, a dozen states, have joined Cambridge Public Schools in the Student Data Privacy Consortium.

- Requiring the same contractual privacy protections from their software vendors.

- Consortium keeps a searchable database of ed-tech software being used by partner districts, including the specific types of data being collected and stored.

- Texas is an active member.

- Cypress-Fairbanks is actively using their membership.

Trusted Learning Environment Seal (TLE) Developed

- Began as an initiative of CoSN (the Consortium for School Networking), in partnership with AASA, the School Superintendents Association, the Association of School Business Officials International (ASBO), and ASCD.

- July, 2015 – Characteristics of a Trusted Learning Environment identified by 28 diverse school system from across the country.

- September, 2015 – CoSN asked 50 technology leaders to validate the identified Trusted Learning Environment practices in 5 areas.

- The TLE Seal is the **only** data privacy seal for school systems, focused on building a culture of trust and transparency.

TLE Recipients

- Baltimore County Public Schools (MD)

- Boulder Valley School District (CO)

- Butler County Schools (AL)

- Cambridge Public Schools (MA)

- Denver Public Schools (CO)

- Fulton County Schools (GA)

- Highland Local Schools (OH)

- Lewisville Independent School District (TX)

- Loudoun County Public Schools (VA)

- Miami-Dade County Public Schools (FL)

- Park Hill Schools District (MO)

- Raytown Quality Schools (MO)

- Round Rock ISD (TX)

- Satsuma City Schools (AL)

- Zionsville Community Schools (IN)

TLE Seal Practices

Leadership Practice: manage and collaborate with stakeholders regarding the use and governance of student data to inform instruction

Classroom Practice: implement educational procedures and processes to ensure transparency while advancing curricular goals

Data Security Practice: perform regular audits of data privacy and security practices and publicly detail these measures

Business Practice: establish acquisition vetting processes and contracts that, at minimum, address applicable compliance laws while supporting innovation

Professional Development Practice: requires school staff to conduct privacy and security training and offer the instruction to all stakeholders

Cypress-Fairbanks ISD Initiatives

- Cybersecurity Specialist is now on staff – James Costello

- Customer Care Center partnered with Cybersecurity team – Eric Pina

- Joined the Texas Student Data Privacy Alliance Consortium.

- Active in state initiatives with Student Data Privacy and Trusted Learning Environment groups

- Enlisted the support of Steve Smith, leading Data Privacy expert and Cambridge Public Schools CIO – workshop held on February 19, 2018

- Members of Infragard and MS-ISAC

- Utilizing multiple resources such as "Living Life Online" from the FTC

Cypress-Fairbanks ISD Initiatives

- Recently received approval for CFISD Data Privacy Agreement.

- CFISD Data Privacy Agreement is being distributed to software vendors with which the district has partnered.

- Information presented to Curriculum Coordinators, Instructional Technology Specialists, and Librarians.

- KnowBe4 software has been purchased and implemented and training campaigns have been distributed to key customers.

- Continuing to update the website to provide resources.

- Evidence gathered to apply for the Trusted Learning Environment Seal in April, 2018.

Cypress-Fairbanks ISD Timeline

Task	Start	Finish	Status
Form state-wide leadership advisory focus group	07/01/17	08/02/17	Completed
Review the requirements and process	08/01/17	08/25/17	Completed
Introduce TLE to Internet Content Filtering Management Governance Committee	11/02/17	11/02/17	Completed
Gather and create artifacts and evidence	11/06/17	04/28/18	Ongoing
Develop or modify artifacts and evidence to mitigate gaps in compliance requirements	01/01/18	04/28/18	Ongoing
Steve Smith assistance gaps in compliance	12/18/18	04/18/18	Ongoing
Present Information to District Support Team (DST)	02/08/18	02/08/18	Completed
Identify and mitigate gaps in compliance	12/18/18	01/30/18	Ongoing
Steve Smith on site workshop	02/19/18	02/19/18	Completed
Share with Instructional Technology Specialists	02/26/18	02/26/18	Completed
Share with Elementary Curriculum Coordinators	2/27/2018	2/27/2018	Completed
Share with Secondary Curriculum Coordinators	3/7/2018	3/7/2018	Completed
Share with Librarians	3/29/2018	3/29/2018	Completed

Cypress-Fairbanks ISD Timeline

Task	Start	Finish	Status
Share with Librarians	3/29/2018	3/29/2018	Completed
Share with Principal Cluster Rep meeting	3/19/2018	4/30/2018	TBD
Share with Curriculum and Instruction ITS	3/19/2018	4/30/2018	TBD
Share with Curriculum Coaches	3/19/2018	4/30/2018	TBD
Complete TLE Application Process	4/26/2018	4/30/2018	Planned
Share with Middle School Roundtable Discussion	4/24/2018	4/24/2018	TBD
Share with Elementary Roundtable Discussion	4/25/2018	4/25/2018	TBD
Share with High School Roundtable Discussion	4/26/2018	4/26/2018	TBD
Provide any required corrections	5/02/2018	5/30/2018	Planned
Share with District Leadership Team Meeting	5/10/2018	5/10/2018	TBD
Share with Assistant Principals	5/11/2018	5/30/2018	TBD
Share with Technology Liaisons	5/11/2018	5/30/2018	TBD
Share with CIC CCIS, IS, and DCs	8/13/2018	8/18/2018	TBD
Share with Teachers	8/13/2018	8/18/2018	TBD
Share with Parents	9/01/2018	9/30/2018	TBD

CFISD Current Status

Leadership

1. The deliberations and decisions of school system leaders reflect an understanding of data privacy and security.

2. The school system has up to date policies and regulations addressing data privacy compliance requirements.

3. The school system's policies and regulations set clear expectations for the protection of student data privacy and security, as well as the transparent use of data.

4. A school system executive leader is identified as the person responsible for development and implementation of data privacy and security policies and practices.

5. School system leaders provide transparent, updated and accessible communications regarding the collection, management and use of student data to their community.

6. School system leaders ensure adequate resources are available to meet data privacy and security needs.

CFISD Current Status

Business

7. The school system has implemented a process for vetting online services for data privacy and security.

8. The school system regularly educates its employees about the importance of, and expectations for, the use of the established vetting process for online services.

9. The school system implements contract language and data sharing agreements addressing student data privacy and data security.

10.   The school system ensures that all business processes associated with student data include enforceable data privacy and security requirements.

CFISD Current Status

Data Security

11.   The school system website includes its data privacy and security policies and practices which are updated as-needed, but at least on an annual basis.

12.   The school system data privacy and security procedures includes information about data retention periods for student records, data transmission technical protocols, data at-rest and methods and controls limiting access to electronic data.

13.   The school system has enforceable policies regarding storage of data on local computers, mobile devices, storage devices and cloud file-sharing and storage services.

14.   The school system utilizes a documented, role-based process when granting access rights to educators, staff, and contractors to data and technology systems.

15.   The school system has a process in place to communicate data incidents to appropriate stakeholders, in accordance with state law and school system policies.

16.   The school system has a business continuity and disaster recovery plan which is verified and tested on an established, regular basis.

17.   The school system performs an audit of data privacy and security practices on an established, regular basis.

CFISD Current Status

Professional Development

18. Privacy and security of student data is embedded into training and professional development in all areas of school operations and academics.

19. The school system provides employees with up-to-date, easily accessible resources and documented processes, including exemplars and templates that facilitate student data privacy and security.

20. Parents are offered awareness training and resources about student data privacy and security.

21. All staff members participate in annual student data privacy training related to applicable federal and/or state laws.

Classroom

22. Teachers implement a curriculum to promote student information literacy, digital citizenship and Internet safety.

23. Teachers are aware of and regularly use the school system's established process for vetting and procuring online services.

24. Teachers model appropriate use and protection of student data for their students.

25. Teacher communications to parents include clear information about the collection, use and protection of student data.

Software Requests - iSupport

- Changes have been made to enable data to be gathered

Software Requests - iSupport

- Changes have been made to enable data to be gathered

Cyberattacks and Security

Insert Web Page

This app allows you to insert secure web pages starting with https:// into the slide deck. Non-secure web pages are not supported for security reasons.

Please enter the URL below.

https:// threatmap.checkpoint.com/ThreatPortal/livemap.html

Note: Many popular websites allow secure access. Please click on the preview button to ensure the web page is accessible.

Web Viewer Terms | Privacy & Cookies   Preview

KnowBe4 Training

Dear JENNIFER MILLER,

In an effort to increase awareness of cyber security threats, you have been enrolled in a KnowBe4 training module.

The courses you've been assigned are displayed below:

- Social Engineering Red Flags

Please use this link to start your training:
https://training.knowbe4.com/login?email=JENNIFER.MILLER@cfisd.net

Please use your CFISD network username and password to complete the sign in process to begin your training.

KnowBe4 Training

KnowBe4 Training

Suspicious Email – Now What?

- Forward the email to iSupport@cfisd.net

- Cc: CyberSecurityAlert@cfisd.net

Suspicious Email – Now What?

Please Read – Important Security Message!

A malicious email was sent to you, from "jim@fakedomain.com"

The subject line was "funny employee list at cyfairisd.com"

The email contained a **<<link to a malicious website/malicious attachment>>**

If you **<<clicked the link/attachment>>**, please contact the Customer Care Center immediately so that we can ensure the computer is not infected. They can be reached at 281-897-4357.

Our email system administrators will be removing the email from all accounts affected by this incident. By the time you see this email, the malicious email may already be removed from your inbox.

If the email is still in your inbox, **do not open it; please delete it right away.**

Thank you for helping to keep the district safe.

Website Updates

- www.cfisd-technologyservices.net
  - Teams
    - Cybersecurity

CFISD Cyber Security Services (CCSS)

The purpose of CCSS is to develop and manage the information (cyber) security program for CFISD. This includes identification and protection of district systems and data through the application of best-practice technological (security tools) and management (policy, process & procedure) as well as monitoring the environment for compliance and response to security threats and incidents.

Student Data Privacy

Cyber Security Current Events

Cyber Security Awareness

Website Updates

- www.cfisd-technologyservices.net
  - Teams
    - Cybersecurity Awareness

Curriculum

TLE Overview

Application Approval Process

Questions?