Woodbridge School District

Technology Plan

2019-2022

Essential Question

How do we create a trusted learning environment that practices and promotes safe and secure data privacy guidelines for the Woodbridge School District?

Abstract

With an ever increasing dependence on technology in school districts, schools need to shift their attention to the use and handling of digital information so that the privacy and security of the individual is respected. Most recently, the primary goal has been to ensure the physical security and safety of individuals in the building, with less focus on the security of new and emerging technologies that are being implemented in the classroom.

The goal of this three year technology plan is to reframe the conversation around student data privacy to one of "trust." Creating this trust requires that school system leaders implement documented compliance policies and practices to protect student data, and that they clearly communicate those policies and practices to, students, parents and the community.

This plan proposes adapting the application for the Trusted Learning Environment (TLE) Seal. TLE is a voluntary program that sets ambitious practices and norms for schools around privacy of student data. Obtaining the TLE Seal would recognize the Woodbridge School District for successfully implementing practices that foster "trusted learning" at the core of their cultures, ensuring faculty and student security. Successfully obtaining the TLE seal, the Woodbridge School District would demonstrate their commitment to high standards and the continuous review of privacy practices.

Past Technology Plan Initiatives

The following initiatives have led Beecher to its current position in technology:

- The *Mobile Computing for Faculty* initiative put a laptop in the hands of every teacher, giving them access to resources, student data, and communications both during school and at home.
- The *SmartBoard* initiative brought interactive digital resources and tools to the front of each classroom for focused instruction.
- The *Mobile Technology for Students* initiative placed iPads into the hands of all students in the classroom, bringing access to digital resources and tools to the places and times when needed most, instead of providing access only at scheduled times in a computer lab.
- The *Beyond the Walls of the School: Empower Continuous Personal Learning* initiative sought to promote personal learning, creativity, and innovation among all members of the Beecher Road School Community, the District supported the needs of the faculty and staff to encourage and nurture students to become independent lifelong learners.

Preface

Technology plans at Beecher Road School for the past two and a half decades have focused the district on leveraging the power of technology to enhance creativity, learning, and productivity. Balanced use of technology has provided many options in the continuously growing toolkit for both students and faculty while students and teachers alike learn to make personal choices from traditional and digital tools.

The previous technology plans have, by necessity, included a primary focus on the acquisition of hardware in quantities adequate to make equal access feasible. The current technology plan now focuses on professional development to optimize the use of these technologies by students, teachers, and administrators for both learning and for managing all the details needed to expand our rich learning environment and programs. At the same time, the plan seeks to insure that the district will continue to replace hardware and provide for services that take advantage of new developments and improvements in our world.

The adoption of PA 16-189 changed the landscape of how technology is used and integrated in classrooms. Therefore, the district must take with a renewed interest a deeper look at how we handle personal information and use it in a safe and secure way. As we are physically entrusted with students, we need to be a trusted steward of their digital information as well. The district needs to reflect on its own data security practices, and also deepen the knowledge and understanding of those practices with staff, parents, and community members.

Components for Successful Plan Implementation

Two of the main components of creating a trusted learning environment are getting buy in from all constituents in the districts as well as developing and understanding the baseline of our needs. The initiative needs to be implemented and supported district wide. All members of the BRS community need to be an active part of the TLE in order for it to take hold and succeed. The technology department will develop a survey for faculty members based on the TLE rubric to obtain a baseline set of data points to analyze the areas of need and begin the process of moving the district towards a more secure technology environment.

The Trusted Learning Environment Program requires school systems to provide evidence and implementation of high standards for data privacy protections around five core areas: Leadership, Business, Data Security, Professional Development and Classroom. To begin this process, the Technology Plan Committee has focused the development of the five areas that will clarify areas of strengths and weaknesses.

Leadership Practices

Beecher Road School will undertake the following to manage and collaborate with stakeholders regarding the use and governance of student data to inform instruction. Members of the Beecher Road School community will:

- Demonstrate an understanding of data privacy and security through the deliberations and decisions of school system leaders.
- Develop up-to-date policies and regulations addressing data privacy compliance requirements.
- Set clear expectations for the protection of student data privacy and security, as well as the transparent use of data through the school system's policies and regulations.
- Identify the person responsible for development and implementation of data privacy and security policies and practices.
- Provide transparent, updated and accessible communications regarding the collection, management and use of student data to their community.
- Ensure adequate resources are available to meet data privacy and security needs.

Evaluation:

- Self assess district progress based on the trusted learning environment rubric
- Evaluate progress and determine areas of need based on rubric scores
- Review communications regarding the collection, management and use of student data to the community.
- Audit and review if adequate resources are available to meet data privacy and security needs.
- Review communications regarding the expectations for the protection of student data privacy and security.
- Review policies and regulations addressing data privacy compliance requirements.

Business Practices

Beecher Road School will undertake the following to acquire and establish vetting processes and contracts that, at a minimum, address applicable compliance laws while supporting innovation. Members of the Beecher Road School community will:

- Implement a process for vetting online services for data privacy and security.
- Educate employees about the importance of, and expectations for, the use of the established vetting process for online services.
- Implement contract language and data sharing agreements addressing student data privacy and data security in compliance with Connecticut's Student Data Privacy laws.
- Ensure that business processes that involve student data privacy and security requirements are in place and enforced.

Evaluation:

- Self assess district progress based on the trusted learning environment rubric
- Evaluate progress and determine areas of need based on rubric scores

- Review the process for vetting online services for data privacy and security
- Review contract language and data sharing agreements
- Review business processes that involve student data privacy and security requirements are in place and enforced
- Review materials and the process/schedule of professional development opportunities provided to employees on the importance of, and expectations for, the use of the established vetting process for online services.

Data Security Practices

To promote data security for all stakeholders of the Beecher Road School community, the district must develop and enforce clear data security policies and practices. Members of the Beecher Road School community will:

- Publish in a publically accessible way its data privacy and security policies and practices which are updated as-needed, but at least on an annual basis.
- Develop district-wide privacy and security procedures which include, at a minimum, of all of the following:
    - defined data retention periods for student records;
    - technical protocols for securing data in transit;
    - physical, technical and administrative safeguards for securing data at-rest;
    - controls limiting access to data.
- Develop enforceable policies regarding storage of data on local computers, mobile devices, storage devices and cloud file-sharing and storage services.
- Implement and utilizes a documented, role-based process when granting educators, staff and contractors access rights to data and technology systems.
- Implement a process in place to communicate data incidents to appropriate stakeholders, in accordance with state law and school system policies.
- Develop a business continuity and disaster recovery plan which is verified and tested on an established, regular basis.
- Performs an audit of data privacy and security practices on an established, regular basis.

Evaluation:

- Self assess district progress based on the trusted learning environment rubric.
- Evaluate progress and determine areas of need based on rubric scores.
- Review policies and procedures developed around the area of data privacy .
- Review templates and drafts of communications related to data incidents.
- Review annually the business continuity and disaster recovery plan.
- Review log/meeting schedules for the audit of data privacy and security practices.
- Review and locate, in a publically accessible way, the data privacy and security policies and practices.

Professional Development Practices

Professional development must provide equal opportunities for individuals to gain and improve the knowledge and skills essential to the security of staff and student data. A successful professional development program ensures that all stakeholders have a voice at every stage of the planning, implementation, and evaluation. Members of the Beecher Road School community will:

- Embed privacy and security of student data into training and professional development in all areas of school operations and academics.
- Provide employees with up-to-date, easily accessible resources and documented processes, including exemplars and templates that facilitate student data privacy and security.
- Offer awareness training and resources about student data privacy and security to parents and the broader community.
- Participate in annual staff student data privacy training related to applicable federal and/or state laws.

Evaluation:

- Self assess district progress based on the trusted learning environment rubric.
- Evaluate progress and determine areas of need based on rubric scores.
- Assess the current security and data privacy needs of the District staff through a self-assessment .
- Survey the staff to determine effectiveness of security and data privacy as well as technology use and proficiency in targeted areas and new initiatives.
- Review professional development surveys and scheduled opportunities in conjunction with the District Professional Development Committee.
- Deliver professional development around the identified needs. Additional support can be provided as needed to small groups and individuals.

Classroom Practices

Classroom practices must ensure transparency while advancing curricular goals when and where needed. Successful classroom practices will implement educational procedures and processes to deepen understanding of online safety and data security practices. To ensure this, over the next three years, members of the Beecher Road School community will:

- Implement a curriculum to promote student information literacy, digital citizenship and Internet safety.
- Develop awareness of and regularly use the school system's established process for vetting and procuring online services to be used in the classroom.
- Model appropriate use and protection of student data for their students.
- Communicate to parents information about the collection, use and protection of student data.

Evaluation:

- Self assess district progress based on the trusted learning environment rubric.
- Evaluate progress and determine areas of need based on rubric scores.

- Review communications to parents about the collection, use, and protection of student data.
- Review school system's established process for vetting and procuring online services to be used in the classroom.
- Review the curriculum created to promote student information literacy, digital citizenship, and Internet safety.
- Develop and review a teacher survey to allow self-evaluation of appropriate use and protection of student data.

Trusted Learning Environment Application

Anticipating readiness to apply for the TLE seal, the District will have shown and provided evidence to support growth in the areas of student data privacy and digital security practices. Evidence of growth through multiple means will validate the commitment the district has made to higher standards of student data safety. To ensure a successful application process, members of the Beecher Road School community will:

- Self assess District progress based on TLE Rubric annually.
- Complete the application for TLE seal.
- Consult with other TLE schools for progress monitoring.

Evaluation:

- Self assess district progress based on the trusted learning environment rubric.
- Evaluate progress and determine areas of need based on rubric scores.
- Submission of the application for TLE seal.

Addendum 1: Goal Timeline

Leadership Practices

Year One:

- Identify the person responsible for development and implementation of data privacy and security policies and practices.
- Set clear expectations for the protection of student data privacy and security, as well as the transparent use of data through the school system's policies and regulations.
- Demonstrate an understanding of data privacy and security through the deliberations and decisions of school system leaders.

On-going:

- Ensure adequate resources are available to meet data privacy and security needs.
- Provide transparent, updated and accessible communications regarding the collection, management and use of student data to their community.

Business Practices

Year One:

- Implement a of a process for vetting online services for data privacy and security.
- Educate employees about the importance of, and expectations for, the use of the established vetting process for online services.
- Implement contract language and data sharing agreements addressing student data privacy and data security in compliance with Connecticut's Student Data Privacy laws

On-going:

- Ensure that business processes that involve student data privacy and security requirements are in place and enforced

Data Security Practices

Year One:

- Develop a business continuity and disaster recovery plan which is verified and tested on an established, regular basis.

- Develop an enforceable policies regarding storage of data on local computers, mobile devices, storage devices and cloud file-sharing and storage services.
- Implement a process in place to communicate data incidents to appropriate stakeholders, in accordance with state law and school system policies.

Year Two:

- The school system data privacy and security procedures include, at a minimum, of all of the following: Defined data retention periods for student records; technical protocols for securing data in transit; physical, technical and administrative safeguards for securing data at-rest; controls limiting access to data.
- Implement and utilizes a documented, role-based process when granting educators, staff and contractors access rights to data and technology systems

Year Three:

- Publish in a publically accessible way its data privacy and security policies and practices which are updated as-needed, but at least on an annual basis.

On-going:

- Performs an audit of data privacy and security practices on an established, regular basis.

Professional Development Practices

Year One:

- Embed privacy and security of student data into training and professional development in all areas of school operations and academics.

Year Two:

- Provide employees with up-to-date, easily accessible resources and documented processes, including exemplars and templates that facilitate student data privacy and security.

On-going:

- Participate in annual staff student data privacy training related to applicable federal and/or state laws.
- Offer awareness training and resources about student data privacy and security to parents and the broader community.

Classroom Practices

Year One:

- Implement a curriculum to promote student information literacy, digital citizenship and Internet safety.
- Develop awareness of and regularly use the school system's established process for vetting and procuring online services to be used in the classroom.

On-going:

- Model appropriate use and protection of student data for their students.
- Communicate to parents information about the collection, use and protection of student data.

Trusted Learning Environment Application

Year Three:

- Complete application for TLE seal

On-going:

- Self assess District progress based on TLE Rubric annually
- Consult with other TLE schools for progress monitoring

Addendum 2: Yearly Goals

Year One:

Leadership Practices

- Identify the person responsible for development and implementation of data privacy and security policies and practices.
- Set clear expectations for the protection of student data privacy and security, as well as the transparent use of data through the school system's policies and regulations.
- Demonstrate an understanding of data privacy and security through the deliberations and decisions of school system leaders.

Business Practices

- Implement a of a process for vetting online services for data privacy and security.
- Educate employees about the importance of, and expectations for, the use of the established vetting process for online services.
- Implement contract language and data sharing agreements addressing student data privacy and data security in compliance with Connecticut's Student Data Privacy laws

Data Security Practices

- Develop a business continuity and disaster recovery plan which is verified and tested on an established, regular basis.
- Develop an enforceable policies regarding storage of data on local computers, mobile devices, storage devices and cloud file-sharing and storage services.
- Implement a process in place to communicate data incidents to appropriate stakeholders, in accordance with state law and school system policies.

Professional Development Practices

- Embed privacy and security of student data into training and professional development in all areas of school operations and academics.

Classroom Practices

- Implement a curriculum to promote student information literacy, digital citizenship and Internet safety.

- Develop awareness of and regularly use the school system's established process for vetting and procuring online services to be used in the classroom.

Year Two:

Data Security Practices

- The school system data privacy and security procedures include, at a minimum, of all of the following: Defined data retention periods for student records; technical protocols for securing data in transit; physical, technical and administrative safeguards for securing data at-rest; controls limiting access to data.
- Implement and utilizes a documented, role-based process when granting educators, staff and contractors access rights to data and technology systems

Professional Development Practices

- Provide employees with up-to-date, easily accessible resources and documented processes, including exemplars and templates that facilitate student data privacy and security.

Year Three:

Data Security Practices

- Publish in a publically accessible way its data privacy and security policies and practices which are updated as-needed, but at least on an annual basis.

Trusted Learning Environment Application

- Complete application for TLE seal

On-going:

Leadership Practices

- Ensure adequate resources are available to meet data privacy and security needs.
- Provide transparent, updated and accessible communications regarding the collection, management and use of student data to their community.

Business Practices

- Ensure that business processes that involve student data privacy and security requirements are in place and enforced

Data Security Practices

- Performs an audit of data privacy and security practices on an established, regular basis.

Professional Development Practices

- Participate in annual staff student data privacy training related to applicable federal and/or state laws.
- Offer awareness training and resources about student data privacy and security to parents and the broader community.

Classroom Practices

- Model appropriate use and protection of student data for their students.
- Communicate to parents information about the collection, use and protection of student data.

Trusted Learning Environment Application

- Self assess District progress based on TLE Rubric annually
- Consult with other TLE schools for progress monitoring