Data Privacy in Education
An iKeepSafe Educator Training Course

Growing concerns about student data privacy can create hurdles for K-12 educators working to expand access to edtech and digital innovations. Today's teachers and administrators need to understand how student personal information is used and improve student privacy protections in order to strengthen parent confidence in digital learning

Student data privacy concerns can create hurdles to expanding access to edtech and digital innovations. Addressing those concerns, and helping parents and others understand how student personal information is used – and protected – is essential. K12 educators have a unique role in managing edtech, student data, and privacy, and in building parent confidence in digital learning.

The iKeepSafe Privacy Courses for educators focus on three objectives:

- *Communicate the importance of balancing innovations in learning with privacy and security responsibilities.*
- *Explain the importance of teaching all students and staff about student data privacy and security.*
- *Describe why everything and everyone who connects to the school network must comply with privacy and security requirements.*

As an educator and an edtech leader, you probably know some of this information already. These materials are designed to help you talk with parents about edtech and students' personal information – and to help colleagues address issues they may face when expanding technology in their classrooms.

Contents

Who should use this Course

All K12 education stakeholders -- including teachers, employees, administrators, and school board members -- play a part in protecting student privacy in the digital world. This training course is designed to give education stakeholders the tools they need to be aware of privacy concerns and keep students safe.

How to use this Course

- Prior to beginning the Training Course, consider organizing a Privacy Professional Development Workshop at your school. Refer to the accompanying Facilitator Guide for talking points and handouts.
- Read and understand each unit's objectives.
- Watch the lesson videos while referring to each accompanying video guide.
- Test your knowledge by completing the Course Quiz.

Objectives of this Course

- Understand your role in protecting student data.
- Recall the basics of student data privacy and educators' legal requirements.
- Identify key competencies necessary to promote digital privacy and safety for students.
- Describe the difference between data privacy and security.
- Recognize the key components required to establish a safe and healthy digital environment.
- Identify the key areas that will help guide digital privacy awareness and compliance.

NOTE:

The video videos in this course document can be accessed by clicking through the links provided in each lesson. This does require an internet connection.

Introduction

If you didn't already watch this video as part of a Student Privacy Professional Development Workshop, watch it now:

Video: Privacy Overview for K-12 Teachers and Administrators

Lesson 1: Introduction to K-12 Data Privacy

Technology is a part of daily life. This is especially true for students, whose educational experiences are enhanced by digital technology. With this innovation, however, comes risks to information privacy and security.

Watch this video for a brief overview of student data privacy, and how it intersects with your role as an educator:

Video Lesson 1 - Teachers Are Heroes: Introduction to K-12 Data Privacy

Lesson 2: Helping Our Heroes - How to be a Data Privacy Hero

Because digital learning is so valuable, it's important to balance learning goals with privacy and security responsibilities. But what do educators need to know? Watch this video for a summary of the key competencies you'll need to develop, including information about key laws governing student information.

Objectives

By the end of this lesson, you will be able to:

- Communicate the importance of balancing technology and learning goals with privacy and security responsibilities
- Identify three key competencies necessary to promote digital privacy and safety for students
- Explain the basics of educators' legal requirements with respect to data privacy

Video Lesson 2 - Helping Our Heroes: How to be a Data Privacy Hero

Watch the video above and follow along using Video guide: Lesson 2 - Helping Our Heroes: How to be a Data Privacy Hero located on the next page.

Video guide: Lesson 2 Helping Our Heroes
How to be a Data Privacy Hero

Follow along with the Lesson 2 video using this guide:

There are many facets to teaching, and all of the pieces must come together for you to reach your goals. You want to help your students to be successful and nurture their love of learning. You use new tools to personalize learning and build on their individual interests. You are their hero. To be confident your students are safe when digital tools are used at school, there are three main concepts you need to understand and apply.

1: Know Where Student Data Goes

When you or your students use digital tools, you leave a trail, much like dropping bread crumbs in a forest. These breadcrumbs in the digital world are bits of digital data.
When information about students is put into a digital tool, it creates a trail of "digital data" or information that can be accessed by others.

So you'll need to ask:

- Who else has access to this data?
- How are they going to use this information?
- Is this information secure?
- Does the process follow privacy law?

Now, you might be wondering, how can we know who has access to this data and what do we need to know about privacy laws?

2: What Data Can Be Shared?

As teachers and educators, it is our job to ensure student information is only used for educational purposes, both for safety and to meet legal requirements. We must know what data can and cannot be shared. For students under 13, this is especially important.

COPPA

- Requires companies to have parent permission before collecting and using the personal information of children under 13.
    - School districts can provide this consent if data is used for educational purposes.
    - Check: Have your digital tools been reviewed for COPPA compliance?

Video guide: Lesson 2 Continued

FERPA

- Parents must give permission for their student's information to be shared.
- Parents have the right to review all education records and information.
- Protects specific student information, like grades, student work, and personal information.
- Allows schools and districts to share "directory information." such as:
  - Student's name, address, phone number, date of birth

When any student information goes into the digital world, you must adhere to FERPA and COPPA. It's also important to check individual state laws!

3: Clear Communication

Setting up clear communication is the backbone to success. Teachers and schools must have clear policies around student privacy, and this information must be shared with parents.

Let them know:

- How these processes work.
- Why these procedures are in place (to ensure protection of students and their personal information.)
- About expectations surrounding appropriate digital conduct.
- How digital tools can enhance learning.

Having all digital products and tools evaluated by a skilled and trusted third party is the fastest and easiest way to ensure that your products comply with data privacy law!

Lesson 3: Reviewing EdTech Products

This lesson has four chapters

Lesson 3, Chapter 1 - Privacy

Student data privacy law requires certain policies and practices for technology products used in educational settings. This lesson provides a general overview of these requirements, so that you can be aware of what types of protections your school's EdTech products must have.

Objectives

By the end of this section, you will be able to:

- Define “privacy policy”
- Explain the basics of privacy compliance for tech products in education
- Identify the key elements needed in a privacy assessment for technology in education

Video Lesson 3 - Reviewing EdTech Products, Chapter 1 - Privacy

Watch the video above and continue following along using Video Guide: Lesson 3 - Reviewing EdTech Products, Chapter 1 - Privacy located on the next page.

Video Guide: Lesson 3, Chapter 1 - Privacy

Before you review the privacy policy, answer these questions:

1. Have you fully reviewed the product for educational use? (Will student data only be used for educational purposes?)
2. Will students be using the product?
3. What educational benefits do you perceive the student receiving from this product? What are the risks?
4. Does the product require adult consent for students under 13 to use?
5. Do you have authority to provide consent?
6. Under COPPA, schools are authorized to provide consent on behalf of parents and may approve a student's use of an educational program.

*An LEA's ability to consent on a parent's behalf is strictly limited to the educational context. That is, an LEA may only consent on the parent's behalf if the personal information collected is used strictly for educational purposes and not for any commercial purpose.**

7. What types of information are being shared?
    a. Is there any information shared that could be considered sensitive?
    b. Are you sharing personally identifiable information?

Review the Privacy Policy

1. Is there a posted privacy policy?
    a. Remember, privacy policies exist to protect companies, not user privacy.
    b. If there is no privacy policy, then you cannot access the information you need to know about what information they will gather and how they will use it. You should use a different product.
    c. If there is a privacy policy, then proceed to question 2.

2. Does it describe all personal information, non-personal information, and/or materials collected or maintained from and about students?
    a. Does it specify whether or not the product, website, online service, or mobile application allows or encourages students to make personal information publicly available, and how that may be done?
    b. Does it provide an explanation of how the information and/or materials are used by the operator?
    c. Does it specify whether or not any of the information and/or materials is disclosed to third parties or partners? Does it include what information might be disclosed, and why?

Video Guide: Lesson 3, Chapter 1 Continued

d. Does it include a statement that that a school has the right to review, have deleted, and/or refuse to permit further collection or use of the student's information? If so, does it include information on how to do so, and the implications for a user refusing collection of data?
e. Does it include verification that the operator will allow for inspection, review, and amendment or changes to student data via an authorized request from a school? Does it provide information on how a school may make such a request?

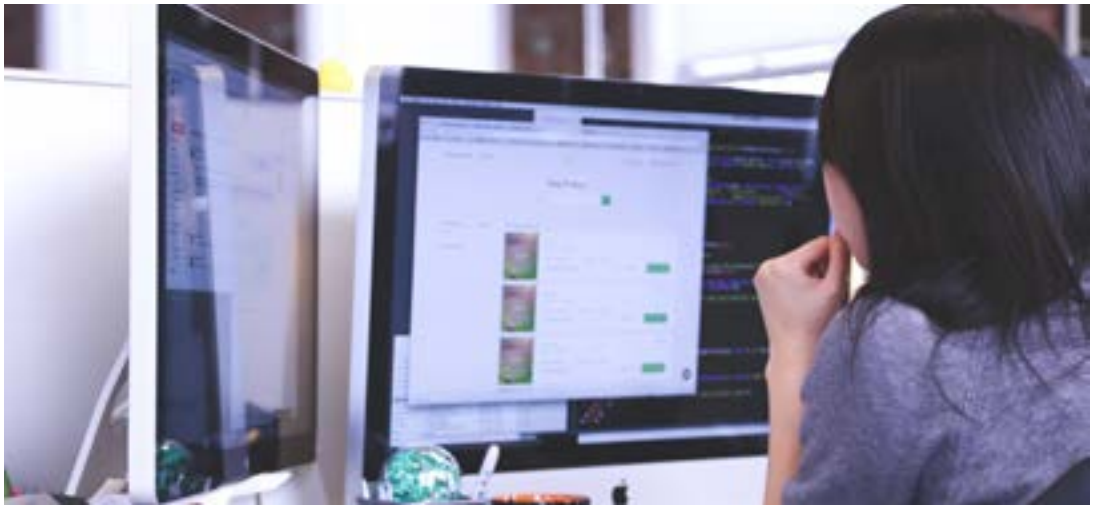
3. Does it include a statement explaining the operator's general practices related to data security and integrity, including any breach of data?

4. Does it give you the ability to contact the operator regarding the privacy policies and use of students' information? (Does it provide a name, address, telephone number, and email?)

Review Advertising Practices

1. Is there an explanation of how ads will be served on the site?
   a. If so, be sure to review it.
   b. Is the operator engaging in targeted advertising?
   (When advertisements are custom-tailored based on information collected, under SOPIPA, operators cannot engage in targeted advertising on their product, website, online service, or mobile application.)

*From "Data Privacy Guidebook" - a collaborative project between the California Education Technology Professionals Association (CETPA), the California County Superintendents Educational Services Association (CCSESA), and Fagen Friedman & Fulfrost



Lesson 3, Chapter 2 - Safety

In addition to privacy and security, technology policy and law provide certain protections for students surrounding the type of content and communications to which they are exposed. This lesson covers the questions and concerns surrounding online safety about which you should be aware when selecting EdTech products.

Objectives

By the end of this section, you will be able to:
1. Define digital safety.
2. Explain the basics of digital safety.
3. Identify the necessary digital safety elements for tech products in education.

Video: Lesson 3 - Reviewing EdTech Products, Chapter 2 - Safety

Watch the video above and continue following along using Video Guide: Lesson 3, Chapter 2 - Safety located on the next page.

Video Guide: Lesson 3, Chapter 2 - Safety

Questions to ask

- Is there a posted Terms of Service? Does it address inappropriate content and conduct?
- Does the TOS state minimum age of users? Do your students meet the requirement?
- Is the product-generated content age appropriate? If present, is the advertising age appropriate?
- Are users generating content? Is content (chat, images, profiles, etc.) moderated?
- Can users communicate with other users (e.g., text, audio, video)?
- What can students share publicly/privately (e.g., images, videos, etc.) and with whom?

Lesson 3, Chapter 3 - Security

Protecting student data requires both administrative and technological security measures, in order to prevent unauthorized parties from accessing it. This section gives an overview of the types of factors you should look for in order to ensure quality data security measures in the EdTech products you use.

Objectives

By the end of this unit, you will be able to:

- Define digital security
- Explain the basics of digital security
- Identify some of the necessary security elements for tech products in schools

Video: Lesson 3 - Reviewing EdTech Products, Chapter 3 - Security

Watch the video above and continue following along using Video Guide: Lesson 3, Chapter 3 - Security located on the next page.

Video Guide: Lesson 3, Chapter 3 - Security

Operators must use and maintain reasonable security procedures and practices, taking into account available technologies and the sensitivity of the data, to safeguard and protect that information from unauthorized access, destruction, use, modification, or disclosure and ensure the confidentiality of personally identifiable information collected from or about students. Such data must be delivered to products in a secure manner and stored securely.

1. Is there a statement within the posted privacy policy explaining the operator's general practices related to data security and integrity including any breach of data?

2. Does the operator meet the following security criteria:
    a. Is student data stored securely? Is sensitive data such as personal information stored separately from other data?
    b. Is student data maintained in a manner that would allow a school access to the data for which it is authorized?
    c. What employees at the company have access to student data?
        i. Access to students' sensitive data, including personally identifiable information, by member company employees is not allowed unless necessary for product operation and educational purposes. In cases where access is necessary, it must be limited to authorized employees, and a procedure must be in place to revoke access when an employee leaves the organization.
        ii. Does the operator conduct background checks on all employees who have access to student data?
    d. How does the company dispose of student data?
        i. A defined process must be in place for securely deleting and disposing of data when no longer needed, inactive data, or when requested by a school or as otherwise noted per the stated terms of use or contractual agreement with a school.
    e. Does the operator conduct security audits?
        i. A defined process must exist for the operator to conduct or have conducted regular security audits. On an annual basis, the operator must allow a school or its designated third party with either access to the results of the Member Company's security audits or with approval to conduct its own security audit of Member Company practices around its data. Schools must have access to the results of audits.
    f. Does the operator have a data breach policy? It should include the following:
        i. Notification Policy and System: Member Company must have in place a notification policy and system containing the following elements:
        ii. Email notification of designated persons of the school district or other educational agency.
        iii. Telephonic notification of designated persons of the school district or other educational agency.

Video Guide: Lesson 3, Chapter 3 Continued

iv. Notification of each user affected by the breach, either separately by the vendor or in conjunction with the school district or other educational agency.
v. Only use operators with such a policy.

3. Contents of Breach Notification: Does the notice answer these questions:

a. What was the date of the breach?
b. What types of information were subject to the breach?
c. Can you generally describe what occurred?
d. What steps is the Vendor is taking to address the breach?
e. Who is the company employee the data holder can contact?
f. How many people were affected by the breach? Some states require notifying the Attorney General's office.
g. If you cannot answer all of these questions from the notice, the notice is incomplete.

4. How are third-party service providers handled?

a. Does the operator have agreements in place with third parties detailing their data privacy and security policies and expectations?
    i. Does this include assurances that third parties are able to comply with these policies?
    ii. Has the operator assessed third-party practices surrounding student data, addressing:
        1. Confidentiality?
        2. Security?
        3. Transfer of personally identifiable information to the school upon request?
        4. Termination of an agreement and data deletion?
        5. Data breach? Does this include a notification process?

Lesson 3, Chapter 4 - Contracts

When entering into or amending a contract with an EdTech vendor, there are several conditions and terms protecting student data that should be included. This section outlines these terms and other concepts you'll need to know when entering into contracts with tech vendors.

Objectives

By the end of this lesson, you will be able to:

- Understand what should be included in a vendor contract
- Understand the outcomes if a contract does not contain all needed information

Video: Lesson 3 - Reviewing Edtech Products, Chapter 4 - Contracts

Watch the video above and continue following along using Video Guide, Lesson 3 - Chapter 4 - Contracts on the next page.

Video Guide: Lesson 3, Chapter 4 - Contracts

Are you entering, renewing, or amending a written contract with the vendor? If so, does the contract contain the following (check your state's specific requirements)?

1. A description of how students can control content created for education-related purposes, along with a way to transfer content to a personal account later.
2. A description of how parents, legal guardians, or students can review and correct personally identifiable information contained in their records.
3. A description of the procedures for notifying affected parents, legal guardians, or eligible students in the event of unauthorized disclosure of student records.
4. A description of how schools and third parties will comply with FERPA.
5. An outline of actions taken by the vendor to ensure security, including designation and training of responsible individuals.
6. An outline of actions that third parties will take to ensure student data is secure and confidential.
7. A statement that the LEA owns and controls student records.
8. A statement that student records will not be retained or available to the third party once the contract is over and an explanation of how that will be enforced.
9. A statement prohibiting third parties from using personally identifiable information from student records to target advertising to students.
10. A statement prohibiting third parties from using student information for purposes outside of those named in the contract.

A contract lacking one of these statements/conditions is nullified. Contracts containing conditions that violate federal or state law are likely invalid as well.

Supplemental Lesson 1 - Privacy & Security Training for School Board Members School Boards Set the Vision

Digital technology is rapidly changing the way we protect student information in school. This course gives school board members the tools they need to be aware of privacy concerns and keep students safe.

Objectives

By the end of this unit, you will be able to:

- Communicate the importance of balancing technology and learning goals with privacy and security responsibilities
- Clarify the difference between data privacy and security
- Contextualize your role as a school board member in protecting student data*
- Identify the key areas that will help guide your school into privacy awareness and compliance

This lesson explains how student data privacy responsibilities intersect with your role as a school board member.

Video: Supplemental Lesson 1 - School Boards Set the Vision

Watch the video above and continue following along using the Video Guide: Supplimental Lesson 1 on the next page.

Video Guide: Supplemental Lesson 1

As a school board leader, you create vision and set direction in education. You ensure accountability and advocate for children, school districts, and schools in the community. Today, one of the most important issues school boards need to address is digital technology. Technology enables innovation and advances learning, but it can also bring risks. Using technology and student data in smart ways can personalize learning experiences and increase efficiency.

What can you do as a school board member?

Tip #1: Understand the landscape — engage with your schools and your community.

Listen to their concerns and investigate the risks your district faces. Having an independent third party conduct a privacy review can help you can identify gaps in your policies and practices and take steps in the right direction.

Tip #2: Understand these important definitions:

- Privacy: The protection of personal information — practices we follow to ensure that data is only accessed by appropriate parties for appropriate uses (including designating permissions).
- Security: Safeguards (which are usually technical) implemented to ensure data is protected (e.g. encryption, strong passwords, etc.).
- Weaknesses in either of these areas can result in a data breach!
  - Most data breaches result from an employee mistake or mismanagement.

Tip #3: Develop your data privacy plan.

You should be able to answer these questions:
1. Who is in charge of student privacy?

- A privacy leader or point person will strengthen practices, ease concerns, and keep things running smoothly.
- A digital privacy and safety team composed of diverse stakeholders will bridge institutional silos, track the pulse of privacy, and inform policy and procedures. This team can include:
  - Teachers
  - Administrators
  - Tech directors
  - Curriculum directors

Video Guide: Supplemental Lesson 1 Continued

2. What kinds of digital tools are being used in your schools?

- What programs, apps, games, and tools are being used in your schools? Have they undergone a privacy assessment?
- Understanding the benefits and privacy practices of these tools will help keep your students safe without sacrificing their competitive education.
- Working with tech vendors is a great way to start!

3. How are the individuals in your schools being trained?

- Do you offer educational resources?
- Training educators, staff, and administrators is essential to complying with the law and fostering a healthy environment.
- Maintaining and understanding this changing landscape can be time-consuming, but will pay out — as understanding grows, each member of the school system becomes a valuable resource!

Once you can answer these critical digital privacy and security questions, you can feel confident that you are helping to foster a positive digital environment. You should circle back with your community, letting them know the good news. Keeping them informed will go a long way toward building confidence and trust.

Supplemental Lesson 2 - Privacy & Security Training for School Administrators Administrators Are Leaders

Digital technology is rapidly changing the way we protect student information in school. This course gives school administrators the tools they need in order to be aware of privacy concerns, and keep students safe.

Objectives

By the end of this unit, you will be able to:

- Communicate the importance of balancing technology and learning goals with privacy and security responsibilities
- Clarify the difference between data privacy and security
- Contextualize your role as an administrator in protecting student data
- Identify the key components required to establish a safe and healthy digital environment

Video: Supplemental Lesson 2 - Administrators Are Leaders

Watch the video above and continue following along using Video Guide: Supplemental Lesson 2 on the next page.

Video Guide: Supplemental Lesson 2

As administrators, you provide leadership and vision in your organization. You train teachers, maintain school safety, and establish educational culture. As leaders, you look for innovative ways to improve education. Digital tools enable innovation, and advance learning, but can also bring risks!

There are new new ways in which student data can be inappropriately used or shared. Here are some tips that will help you navigate the new digital terrain:

Tip #1: Protecting the digital privacy of your students means more than just securing education records.
All kinds of information, such as name, email address, date of birth, and even IP address, have new and digitally-specific protections.

Tip #2: Because digital tools are critical to maintaining a competitive education in today's world, protecting privacy doesn't mean abandoning technology altogether, but using it in smart and safe ways.
Balancing digital learning with privacy and security is essential to fostering a successful digital culture.

Tip #3: Understand these important definitions:

Privacy - The protection of personal information — practices we follow to ensure that data is only accessed by appropriate parties for appropriate uses (including designating permissions)

Security - Safeguards (which are usually technical) implemented to insure data is protected. (e.g. encryption, strong passwords, etc.)

A Positive Digital Culture - An environment in which technology is used in healthy and safe ways. All actors and stakeholders have an understanding of what behaviors and practices are appropriate to maintain this environment.

- What does this environment look like? Think about student safety on campus (in the physical world): Educators, staff, and administrators already have an understanding abou when student information should and shouldn't be disclosed, and what kind of behavior is appropriate - this kind of understanding should be rejected in the digital world!

You might be wondering: **What can I do to protect student data?**
Well, you play the most critical role in your school — **it is your job to know where your students' data goes and who has access to it.** One aspect of this is compliance with privacy law -- you must ensure that all technology products in your school, including games, administrative tools, and more, properly follow the law. You should have tech vendors' policies and practices reviewed to make sure they meet their specific requirements.

Video Guide: Supplemental Lesson 2 Continued

Your efforts should focus on four key domains: **Policies, Programs, Systems,** and **Incident Response plans**

1. Policies

- Assemble a Digital Privacy and Safety Team — a group of diverse stakeholders from all across the educational community
  - Ex: Teachers, Curriculum developers, Administrators, IT directors, Community leaders, etc.
  - Bridging institutional silos will serve as a huge advantage when developing your policies and procedures.
- Policies should clearly and accessibly articulate the privacy practices that your school will follow, including how personal data will be collected, maintained, used, and protected.

2. Programs

- Your data privacy initiative should include a comprehensive data privacy program, including:
  - Identifing and minimizing privacy risks
  - Documenting an incident response plan
  - Updating policies in light of changing technologies and law
  - Educating employees and student about privacy skills and competencies
  - Informing the community about privacy rights and responsibilities

3. Systems

These should account for two components:

- **Access**: Only those who need data for educational reasons should be able to access it.
- **Security**: Your cybersecurity measures should be up to date, taking into account available technologies.

An independent third party review can help you take steps in the right direction.

4. Incident Response Plans

Understand your legal requirements in the event of a data breach or other digital incident

- Weaknesses in either privacy or security practices can result in data breaches.
- No matter what the cause of the breach is, your response must be the same, following all reporting requirements.

Once you've achieved these goals, be sure to maintain them. It's sort of like going to the doctor - you may go when you're sick, but you also return for regular check-ups, to make sure everything is still working as it should. If you keep up the good work in the long-term, your students and community will reward you with their confidence and trust.

Additional Resources:

FERPA 101 for Educators:
The Family Educational Rights and Privacy Act of 1974 is a federal law that protects student educational records. Review the circumstances under which educational records can be released, to whom, and what information can be included.

COPPA 101 for Educators:
The Children's Online Privacy Protection Act is a federal law protecting student data from commercial technology operators. This document summarizes the basics of COPPA and privacy, and helps K12 educators consider ways to build parent confidence about education technology and protections for personal information of young students.

Protected Student Data Table:
There are many different kinds of information that are protected under federal and state privacy law. This table outlines the different types of data you should be especially careful gathering or sharing. The state laws listed are those of California; be sure to check your state's specific requirements.

Top 10 Privacy Tips For Educators:
This document walks educators through likely scenarios where student privacy needs to be considered. It is designed to increase student privacy awareness and improve privacy practices. This document also provides background information on important regulatory issues and how educators should navigate the balance between managing helpful student information and respecting student privacy.

Find iKeepSafe Trusted Products:
The products on this page have been assessed by iKeepSafe and are recognized as compliant with federal and state privacy laws. Find products that meet our rigorous standards.

iKeepSafe Privacy Curriculum Matrix K-12 BEaPRO™:
provides a comprehensive and sequential approach to teaching privacy skills.

The Safety, Privacy, and Digital Citizenship High School Curriculum:
Created in partnership with the Berkman Center for Internet & Society at Harvard University, a comprehensive guide to teaching age-appropriate online privacy and safety skills and competencies. Find more on the Berkman Center's Digital Literacy Resource Platform.

Third Party Certification Request Email Template
Use this handy email template to send to technology companies requesting that they earn third party data privacy certification of their products.

About iKeepSafe

Founded by Jacalyn S. Leavitt, former First Lady of Utah, in 2005, the Internet Keep Safe Coalition (iKeepSafe) certifies digital products as compliant with state and federal requirements for handling protected personal information. We help organizations achieve and maintain compliance through product assessments, monthly monitoring, annual training, and assistance with remediation.

iKeepSafe works with parents, educators and others to ensure that kids thrive in an increasingly digital world. We have a long history collaborating with schools, and we want to help all stakeholders in the K12 education community in their role as stewards of student information in the digital era.

Our Mission

The iKeepSafe mission is to provide a safe digital landscape for children, schools, and families by supporting the protection of student privacy, while advancing learning in a digital culture. To support this mission, we provide data privacy certifications to technology companies, educational resources to schools, and information to the community.

Data Privacy Certifications

iKeepSafe currently provides technolocy companies with assements and certifications for their products for federal and state data privacy laws.

The iKeepSafe FERPA Certification demonstrates compliance with the federal mandates as well as iKeepSafe's rigorous guidelines.

The iKeepSafe COPPA Safe Harbor Certification program ensures that practices surrounding collection, use, maintenance and disclosure of personal information from children under the age of 13 are consistent with principles and requirements of the Children's Online Privacy Protection Act (COPPA).

The CSPC Certification builds on iKeepSafe's FERPA Assessment and COPPA Safe Harbor, assessing for federal and California laws governing student data privacy.

An Certification from a trusted and experienced independent third party like iKeepSafe assures schools and parents that educational technology products can be trusted with handling student data.

Look for the iKeepSafe Data Privacy Certification badge when making your school's technology decisions.

Glossary of Terms

Children's Online Privacy Protection Act (COPPA): The Children's Online Privacy Protection Act of 1998 (COPPA) is a federal law designed to help parents remain in control of what personal information websites and other online services can collect from their young children.

COPPA is administered by the Federal Trade Commission (FTC). It applies to operators of websites, apps, or other online services that collect, use, or disclose personal information from children under the age of 13, and to operators of general audience websites, apps, or online services that have actual knowledge that they are collecting, using, or disclosing personal information from children under 13.

Related Terminology:

Child: A child means an individual under the age of 13.

Collects or collection: Collects or collection means the gathering of any personal information from a child by any means, including but not limited to:

- Requesting, prompting, or encouraging a child to submit personal information online;
- Enabling a child to make personal information publicly available in identifiable form. An operator shall not be considered to have collected personal information under this paragraph if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete such information from its records; or passive tracking of a child online.

Disclose or disclosure: Disclose or disclosure means, with respect to personal information: The release of personal information collected by an operator from a child in identifiable form for any purpose, except where an operator provides such information to a person who provides support for the internal operations of the Web site or online service; and making personal information collected by an operator from a child publicly available in identifiable form by any means, including but not limited to a public posting through the Internet, or through a personal home page or screen posted on a Web site or online service; a pen pal service; an electronic mail service; a message board; or a chat room

Obtaining verifiable consent: Obtaining verifiable consent means making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child:

- Receives notice of the operator's personal information collection, use, and disclosure practices; and authorizes any collection, use, and/or disclosure of the personal information.
- Personal information: Personal information means individually identifiable information about an individual collected online, including:
    - A first and last name;
    - A home or other physical address including street name and name of a city or town;
    - Online contact information as defined in this section;
    - A screen or user name where it functions in the same manner as online contact information, as defined in this section;
    - A telephone number;
    - A Social Security number;
    - A persistent identifier that can be used to recognize a user over time and across different web sites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier;
    - A photograph, video, or audio file where such file contains a child's image or voice;
    - Geolocation information sufficient to identify street name and name of a city or town; or Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

Family Educational Rights and Privacy Act (FERPA):
FERPA is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Related Terminology

Student: A student is any individual who is or has been in attendance at an educational agency or institution and regarding whom the agency or institution maintains education records.

Education records: Education records are those records that are directly related to a student and are maintained by an educational agency or institution or by a party acting for the agency or institution.

Directory Information: Directory information is information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed. Typically, "directory information" includes information such as name, address, telephone listing, date and place of birth, participation in officially recognized activities and sports, and dates of attendance. A school may disclose "directory information" to third parties without consent if it has given public notice of the types of information which it has designated as "directory information," the parent's or eligible student's right to restrict the disclosure of such information, and the period of time within which a parent or eligible student has to notify the school in writing that he or she does not want any or all of those types of information designated as "directory information."

Eligible Student: Eligible student is a student who has reached 18 years of age or is attending a postsecondary institution at any age. This means that, at the secondary level, once a student turns 18, all the rights that once belonged to his or her parents transfer to the student. However, a secondary school or postsecondary institution may still provide an eligible student's parents with access to education records, without the student's consent, if the student is claimed as a dependent for IRS tax purposes.

Personally Identifiable Information (PII): PII includes information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information.
School Official: School official means any employee, including teacher, that the school or district has determined to have a "legitimate educational interest" in the personally identifiable information from an education record of a student. School officials may also include third party contractors, consultants, volunteers, service providers, or other party with whom the school or district has outsourced institutional services or functions for which the school or district would otherwise use employees under the school official exception in FERPA.

General Security Terms

Data Breach: A data breach is the intentional or unintentional release of secure information to an untrusted environment.

Secure File Transfer Protocol: Secure file transfer protocol is a broad term referring to network technology used to encrypt authentication information and data files in transit, so that data files can be safely accessed, transferred, and managed.

Transport Layer Security (TLS): TLS is a cryptographic network protocol that provides authentication confidentiality, and data integrity between two communicating applications. TLS is used as a mechanism to protect sensitive data during electronic dissemination across the Internet.

Data Security: Data security is the means of ensuring that data are kept safe from corruption and that access to it is suitably controlled. The primary goal of any information and technology security system is to protect information and system equipment without unnecessarily limiting access to authorized users and functions.

Data Stewards: Data stewards are managers and administrators within an organization who are responsible for implementing data governance policies and standards and maintaining data quality and security.

References:
Indiana University and US Government Publishing Office

Data Privacy in Education

An iKeepSafe Educator Training Course

Facilitator Guide

Designed to accompany the Data Privacy in Education - An iKeepSafe Educator Training Course, this Guide will help administrators or teachers prepare a Student Data Privacy Professional Development Workshop for their school teams.

Purpose of the Facilitator Guide

These materials are designed to accompany the Data Privacy in Education - An iKeepSafe Educator Training Course. This Guide will help administrators or teachers prepare a Student Data Privacy Professional Development Workshop for their school teams -- including teachers, employees, administrators, and school board members. Its purpose is to serve as a kick-off to the Training Course; facilitators will discuss key aspects of privacy in education with their school teams, underscoring why it is important that each member of the school team understand how data privacy in education has evolved as well as current privacy and security requirements. Although this workshop is intended for school teams who have not yet completed the Training Course, we recommend that the presenters take time to read through all of the handouts as well as complete the Training Course prior to leading this discussion so that they are better equipped to lead the discussions and answer questions.

Objectives of this Course

- Communicate the importance of balancing innovations in learning with privacy and security responsibilities.
- Explain the importance of teaching all students and staff about student data privacy and security.
- Describe why everything and everyone who connects to the school network must comply with privacy and security requirements.

Delivering Your Student Privacy Professional Development Workshop

You will need:

- **Data Privacy in Education - An iKeepSafe Educator Training Course**
- **PPT**: Student Privacy Professional Development Workshop
- **Handout 1:** Protecting Student Privacy and Advancing Learning: How Technology and Data are Improving Schools and Learning
- **Handout 2**: Protecting Student Privacy and Advancing Learning: Building Trust with Parents and Community
- **Handout 3**: Protecting Student Privacy and Advancing Learning: Educators are Stewards of EdTech, Data, and Privacy
- **Handout 4**: Privacy Lead Objectives

(Handouts can be found within this packet, or downloaded from the links above.)

Run of Show

1. Introduction: Why Do We Use Digital Technology?

- Share Handout 1: Protecting Student Data Privacy and Advancing Learning: How Technology and Data are Improving Schools and Learning
  - Read the handout as a group (Note: for large groups, we recommend that you break into smaller groups to read through it.)
  - Discuss benefits of EdTech and personalized learning
    (For example, instruction can be paced according to learning needs, tailored to learning preferences, and tailored to the specific interests of different learners.)

2. Education & Privacy Laws

- Show Video: Privacy Overview for K-12 Teachers and Administrators
- Share Handout 2: Protecting Student Privacy and Advancing Learning: Building Trust with Parents and Community
  - Read the handout as a group
    (Note: for large groups, we recommend that you break into smaller groups)
  - After reviewing the document, discuss as a group by asking these questions:
    1. What are the laws protecting privacy and what exactly is protected?
    2. How are parent concerns/interests reflected in these laws?
    3. Why is it important to develop privacy practices with student information?
    4. Who is responsible and who is affected?

3. EdTech and Student Information

- Continue the discussion by asking these questions:
  1. How do digital platforms use information?
  2. How do digital platforms deal with security and privacy?
  3. What are the risks of failing to protect students in the digital world?

4. Developing Best Practices for Privacy and Security

- Share Handout 3: Protecting Student Privacy and Advancing Learning: Educators are Stewards of EdTech, Data, and Privacy
  - Read the handout as a group
    (Note: for large groups, we recommend that you break into smaller groups)
  - After reviewing the document, discuss as a group by asking this question:
    What is one key takeaway for you personally from this handout?

Run of Show Continued

5. Introduce the Educator Training Course

- Participants can find the Data Privacy in Education - an iKeepSafe Educator Training Course online at iKeepSafe.org/privacyeducation.
- Facilitators have several options for administering the course:
  - Send participants away with the Training Course to complete individually
  - Go through the training course as a group by watching the videos and going through the video training guides together
  - Break into groups by educator role (administrators, educators, board members) to complete the Training Course
- It is recommended that all participants complete the **online exam** following the course
- Consider reconvening as a large group to share your scores with each other, and/or offering an incentive for achieving a high score.

5. Wrap Up and Q&A

Next Steps After the Initial Workshop

- Set a deadline for the Training Course to be completed.
- Consider planning a follow up meeting to discuss key takeaways (as mentioned above).
- Establish an E-Safety Committee and Privacy Lead. (Handout 4: Privacy Lead Objectives)
- Evaluate current EdTech products and resources. (iKeepSafe's resources are available to help ease the burden for educators.)
- Find a list of approved products at ikeepsafe.org/products/
- Recommend a product to be approved (see email templates provided in the Training Course).

Handout 1

Protecting Student Privacy and Advancing Learning
How Technology and Data Are Improving Schools and Learning

Student data privacy concerns can create hurdles to expanding access to EdTech and digital innovations. Addressing those concerns, and helping parents and others understand how student personal information is used – and protected – is essential. K-12 educators have a unique role in managing EdTech, student data, and privacy, and in building parent confidence in digital learning.

How are technology and personal information improving learning for individual students?

Digital technology brings new tools to help teachers personalize and improve learning for students. In addition, new evaluation tools can make grading more efficient, so that teachers can spend more time with students. Teachers work hard to help each student learn at his or her own pace – encouraging students who have mastered a subject to move further, giving extra support when needed, and keeping all students engaged. Detailed personal information helps teachers identify strengths and gaps for each student, and connect a student to challenging but achievable learning experiences that build on his or her personal interests.

Education doesn't work with a "one size fits all" approach, and technology gives us more opportunities to meet the needs and interests of students. Personal information and individual feedback are also crucial for evaluating new EdTech tools, and making sure they continue to help you inspire and support students.

How are technology and personal information improving schools and tools?

Quality data brings valuable feedback about how new teaching practices and tools work, including with specific groups of students, such as English language learners. Reliable data help us highlight and share best practices from a successful teacher or school. For more examples, take a look at What is Student Data? from DataQualityCampaign.org.

The Internet and technology help educators develop new approaches in classrooms and schools, and learn from innovations in other schools. Smart use of data helps you compare ideas and choose approaches that help your students learn, and help your schools manage resources more effectively.

You need to ensure that students – and educators – are prepared to make the most of the Internet and technology. That includes finding the best tools to support learning, and making sure students' personal information is protected.

This is not legal advice. For detailed legal information on student privacy issues, talk with your school attorney or review information such as http://www.f3law.com/privacy.

For more information on iKeepSafe Data Privacy Certified Products, visit https://ikeepsafe.org/products/

Handout 2

Protecting Student Privacy and Advancing Learning
Building Trust with Parents and the Community

Student data privacy concerns can create hurdles to expanding access to EdTech and digital innovations. K-12 leaders need to address these issues and help parents and others understand how student personal information is used – and protected – in order to strengthen parent confidence in digital learning. Communicating effectively with parents starts with understanding these concerns.

Why are some parents concerned about student privacy?
Different parents have different concerns about privacy and student information. Some parents worry about data breaches and ID theft, while others may be more concerned about online tracking and targeted advertising. Some parent concerns may actually be tied to other issues, such as opposition to standardized testing. Appreciating why parents are concerned is the first step toward addressing their concerns and building trust. (One good illustration of parent perspectives on potential benefits and risks involving technology, student data, and privacy is a 2015 survey by the Future of Privacy Forum.)

It's also essential to help parents understand how technology and personal information can improve learning – including in ways they may already see, such as providing better information for parent-teacher conferences, which helps us work together to support learning.

Do technology and use of personal information increase risks of data breaches and ID theft?
Data breaches are in the news regularly, creating a growing awareness of potential dangers, including ID theft. Kids may face even greater risks from ID theft because they don't usually check their credit until they are older, so if their personal information is stolen, thieves have more time to damage their credit or reputation.

ID theft and data breaches are serious issues, and it's essential for teachers and administrators to build strong, secure systems to protect personal information, and to make sure parents know that these systems are in place. Also, everyone (including parents and students) needs to recognize secure systems begin with each of us, including– using strong passwords and taking other steps to protect our information, as well as respecting the information of others.

Risks of data breach and ID theft are also reasons to educate children about financial literacy. As soon as young children start learning about money and math, we can start helping them appreciate the value of their personal information, and steps they can take to protect it.

How do you talk with parents who are worried about EdTech and advertising?
We've all experienced the ways in which Internet tools collect our information (sites we visit, stories we click, geolocation) and use it to suggest things that may be interesting, such as nearby restaurants, suggested movies, weather or traffic information – and advertising. Online tracking and advertising may bring some benefits for adults, but targeting advertising and

Handout 2 Continued

content at kids brings risks. For example, kids may see ads that reinforce negative feelings about body image, or encourage smokingand other unhealthy behaviors.

In addition, some parents and advocates feel that it is unfair to use students' education information to drive advertising. New laws in some states reflect these concerns, and prohibit using education information for targeted advertising or marketing. This is a reasonable goal, but legislation alone may have limited impact. For example, some apps and tools used in schools today (e.g., email or Minecraft) are not designed exclusively for educational purposes, so they may not be covered by new laws.

As schools expand Internet access, students will see more online ads, but they may not be targeted using personal information. Some advertising is contextual, such as sporting gear ads that appear when you visit a sports site. Internet companies rely on advertising – targeted, contextual, and otherwise – and using the Internet means we all see more ads, even if marketers can't use student information. When parents are concerned about advertising, it may help to suggest ad blocking services for their kids' devices. It's also important to teach digital literacy, and help students identify and decode online ads, sponsored content, and other marketing tools.

In addition, help parents recognize that most kids have personal information online in part because of what they and their families do at home. Many kids' online presence begins at a young age, when their parents share photos and information through social media. Personal information moves in many ways through many platforms, and protecting it involves many steps – more than just laws restricting the use of education information.

Different families have different concerns about children's information.
Since parents have different concerns about privacy, some federal and state laws focus on empowering parents to decide whether their children's personal information is collected and used:

- FERPA (the Family Educational Rights and Privacy Act) limits how schools can use and share student education records, and establishes when they need permission from a parent or an adult student. (There are exceptions for school officials using information for educational purposes.) FERPA also gives parents and adult students the right to review a student's education records. For more information, visit the US Department of Education's Privacy Technical Assistance Center or the Data Quality Campaign guide on Student Data Use.

- For kids under 13, COPPA (the Children's Online Privacy Protection Act) requires online sites and services (including apps) to get parental consent before collecting or using any personal information. For more information, visit the Federal Trade Commission and iKeepSafe's COPPA Safe Harbor page.

Handout 2 Continued

- Some new state laws prohibit online sites and services from using student education information for certain types of advertising and marketing. The Data Quality Campaign has a good summary of legislation that states have recently passed or debated .

While COPPA and some state laws apply primarily to online companies, they can also impact schools and educators because you may be sharing student information with a company by using EdTech products or services. These laws are another reason to inform parents about digital tools in your classroom, so that they are more prepared to make decisions regarding technology and their kids' personal information.

Parents have different views on privacy, just like they have different ideas about education. Concerns may vary because of the age of their children, comfort with technology, and other factors. Educators see these differences in your community every day, and you appreciate how your community may view things differently from another city or state. This is one reason why it's hard to craft one set of rules about education privacy and technology. It's also why your role in these conversations is so important – because you understand the views of your families, and your families respect and appreciate your efforts to bring the best resources to their children.

Technology makes student information and privacy more complex for educators.
When FERPA was written in 1974, most student education records were paper documents kept in filing cabinets. Even a few years ago, most electronic information about students was on a server in a locked closet in a school office. Today, schools use multiple vendors for education services, and technology in classrooms uses more personal information. These new services can help personalize learning, and improve data security (cloud services are often more secure than older district networks) but they can also change how you manage student information at the school and district level.

Handout 3

Protecting Student Privacy and Advancing Learning
Educators Are Stewards of EdTech, Data, and Privacy

Student data privacy concerns can create hurdles to expanding access to EdTech and digital innovations. Addressing those concerns and helping parents and others understand how student personal information is used – and protected – is essential. K-12 educators have a unique role in managing EdTech, student data, and privacy, and in building parent confidence in digital learning.

Why do educators need to focus more on data privacy and security?
For decades, educators have been protecting student information, ensuring that it is used for educational purposes. Today, technology generates more information (e.g. geolocation data, IP address, unique identifiers, etc.) and provides more ways to share it. Therefore, when confidential student information (such as grades, medications, mental health issues, learning gaps, family custody) is digitized, it needs even stronger protections.

As leaders bringing technology into schools, you need to understand how new tools and platforms use student personal information. You need to know where data goes, and ensure that your vendors and partners have appropriate policies and protections in place. You teach students to be digital citizens – to understand and manage their digital footprints. You need to understand and manage your data footprints in the same way.

As an EdTech leader in your school, you're an essential voice on these issues.
You know technology can help students succeed. As a leading voice in your school community, you need to promote and model smart technology and privacy protection. Your ability to communicate and build trust with parents is essential to expanding innovation in classrooms. Communicating about EdTech and privacy is a great way to engage parents – and to meet your obligation to notify them about their FERPA rights.

Building your student privacy protection program.
Crafting the right policies, procedures, and training will significantly reduce the risk of privacy mistakes that can hurt your students, your schools, and your community relationships. A strong privacy program helps you identify and reduce risks, and prepares you to respond when incidents occur.

- Get everyone involved. Think about all the educators in your school or district who should be on the team building your privacy policies and practices. Engaging people early builds support for the process – and the results.
- Establish a privacy lead. The team is essential, but you need one point person at your school or district – a CTO, a CPO, an EdTech leader – prepared to respond to questions from colleagues, parents, or students.
- Review what you're already doing. Are there gaps to address? Have breaches or other problems occurred? Exploring previous incidents can help you establish a roadmap and

Handout 3 Continued

build a comprehensive and coordinated approach.
- Build best practices for managing vendors, apps, and devices.

When you choose third-party vendors and services that use student information, you need to make sure they understand your school's legal obligations to protect and secure the data, and that they have appropriate policies and practices in place. Review how a vendor will use, store and protect information, and who will have access to information – at the company and at your school. Also, your school or district legal counsel should be involved in negotiating contracts with vendors.

There's a growing push to require EdTech vendors and developers to get parent permission for using student information, and to explain clearly how the information will be used. (Some new state laws include these requirements.) It's a good idea to find vendors, products, and apps that make clear how they will – and won't – use student information. Look for products that have received iKeepSafe Privacy Assessments. But remember: Parents still see you and your school as primarily responsible for protecting student information.

Using more tablets and devices (school-owned or Bring-Your-Own-Device) in schools means you need to consider how they collect and use student information. Devices created for general use may not meet higher standards for protecting student information. You need to understand how tools can increase the risk of data breaches or other privacy problems.

Use education as the keystone of your privacy program:
Great policies and practices are essential, but education is the best way to strengthen every part of your privacy program. Teach students about protecting their own personal information and respecting the privacy of others. Social media and messaging apps are key places for students (and adults) to remember core tenets of digital literacy and citizenship, including respect for privacy and safety. You can find great digital literacy and citizenship resources from the Harvard University Berkman Center Digital Literacy Resource Platform and Digital Citizenship Institute's whitepaper, "Digital Citizenship - A Holistic Primer".

Educate parents about the strong privacy program you've built and about steps they can take to protect their kids' information. Educators and families all want to advance learning and protect privacy, and as we expand the ways we use technology – in school, at home, and in between – we all share a role in balancing innovation and protection.

"It is essential that children learn about data privacy and security. Their lives will be fully enveloped by technologies that involve data. But far too little about these topics is currently taught in most schools." – Daniel Solove, Professor of Law, George Washington University Law School, and Founder, TeachPrivacy

Handout 4

Privacy Lead Objectives
e-Safety Committee

Objective 1: Educate the individuals in your institution:

- How digital platforms access and use information
- How digital platforms handle security and privacy
- Importance of privacy practices with student information
- Risks of noncompliance with student practices, privacy law, and policy
- Process being developed to adopt best privacy practices with student information

This first objective will take the longest to accomplish and is also extremely important. Because most people do not understand how digital privacy works or how digital data is stored and used, the first step is to teach them. Through workshops, presentations, or training seminars, your organization has to educate all of its members about the use of digital platforms in education, the challenges and risks presented around protecting the privacy of student information, the risks of all non-compliant digital platforms, and why it is important to foster a positive digital culture.

Objective 2: Evaluate current practicesWhat digital platforms are being used in class or are related to students in any context?

- Who is putting in student information and what is the current protocol for recording all forms of student information?
- Which digital platforms do we use most often and therefore need to be evaluated first? What is the order, in terms of priority, that the remaining platforms will need to be evaluated?
- What new practices do we need to adopt to best promote privacy protection?

This second objective will require less time to accomplish than the first objective but is also critical to success. Because members of your organization now understand the risks of digital platforms and privacy, they will be the most valuable part of your team when identifying what noncompliant digital technology is being used. They can identify important practices like what apps they use, what programs and platforms individual sites use, and where the connections between student information and record keeping most frequently occur. Once you have accomplished this objective by gathering all of the related information, you are ready to work on the next step.

Objective 3: Certify

- Have all current products evaluated with a manual and technical assessment to ensure that privacy policies and practices align and contracts are compliant. (For example, you could suggest that their products become iKeepSafe Certified)
- Identify and use the best digital products with regards to data privacy.

For the last objective, you will develop a process to make sure the best privacy compliant products are used. This requires systematically phasing out products that are not safe and secure, and replacing them with products that are.

This is not legal advice. For detailed legal information on student privacy issues, talk with your school attorney or review information such as http://www.f3law.com/privacy.

For more information on iKeepSafe Data Privacy Certified Products, visit https://ikeepsafe.org/products/

Data Privacy in Education
An iKeepSafe Educator Training Course

This training course is designed to give education stakeholders the tools they need to be aware of privacy concerns and keep students safe.

Who Should Take This Course?

All K12 education stakeholders:

- Teachers
- Employees
- Administrators
- School board members

Go to previous page

The Data Privacy in Education Educator Training Course is a comprehensive training program providing tools to equip education stakeholders with necessary knowledge about student data privacy. The course takes a deep dive into the requirements of schools and technology vendors. It is meant to be a resource that gives educators and schools confidence in making technology choices and protecting data.

Find more information on data privacy for teachers and technology vendors here.