DATA PRIVACY AND GOVERNANCE 101

—

REQUIRED TRAINING FOR ALL Talladega County Schools Employees

Why a Data Governance Policy?

In 2013, and in response to an increasing amount of data being collected both electronically and in hard copy, the State Board of Education of Alabama implemented a requirement that all local boards of education have a Data Governance Policy that addresses areas seen as critical in safeguarding student ***personally identifiable information (PII).***

Why a Data Governance Policy?

FERPA - (Federal Education Right to Privacy Act of 1974) gives parents access to their child's education records, an opportunity to seek to have the records amended, and some control over the disclosure of information from the records. With several exceptions, schools must have a student's consent prior to the disclosure of education records *after that student is 18 years old*. The law applies only to educational agencies and institutions that receive funding under any program administered by the U.S. Department of Education.

The Big Picture

It is the policy of Talladega County Schools that data or information in all its forms--written, electronic, or printed--is protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment, software, and practices used to process, store, and transmit data or information.

Talladega County Schools Data Governance Policy

Outlines how operational and instructional activity shall be carried out to ensure Talladega County Schools' data is accurate, accessible, consistent, and protected.

The document clearly establishes who is responsible for information under various circumstances and specifies what procedures shall be used to manage and protect it.

The Talladega County School District follows all local, state, and national laws: The district will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems.

What does DATA GOVERNANCE MEAN?

Data Protection and Privacy

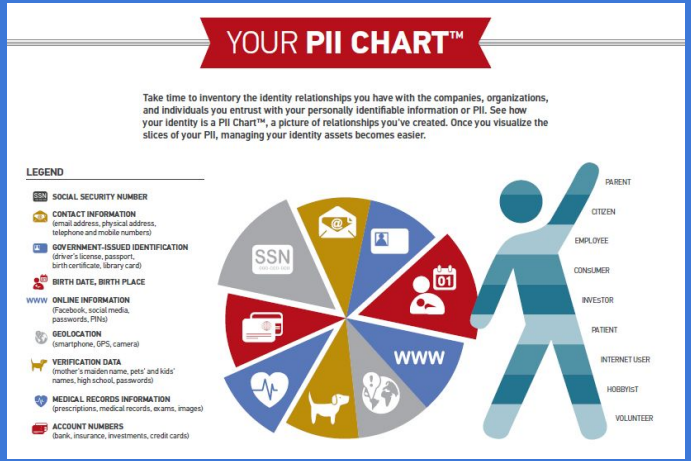
Ensuring the security of sensitive and personally identifiable information (PII) and mitigating the risks of **unauthorized disclosure**

Data Security

In its most basic definition, data security means protecting information and information systems from **unauthorized access**, use, disruption, or destruction

What Constitutes PERSONALLY IDENTIFIABLE INFORMATION (PII)?

Information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; and information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates



How Can We Protect Data and Privacy?

Strategies Already in Place or Being Implemented in the Future

- Provide a website with data policies
- Provide guidelines for all contracts and MOAs that involve data
- Review of the Laws
- Train staff on data governance, privacy, and security
- Make students aware
- Incorporate secure means for accessing data files
- Incorporate secure means for sharing and storing data

How Can We Protect Data and Privacy?

Strategies Already in Place or Being Implemented in the Future

Enforce mandatory password changes

Update, maintain, and monitor firewall

Update, maintain, and monitor virus protection

Update, maintain, and monitor Internet filtering

Backup key data to off-site server

All Employees Must Be Trained

How often?

ANNUALLY

What kind of data is protected by the Data Governance Policy?

- Speech, spoken face to face, or communicated by phone or any current and future technologies
- Hard copy data printed or written
- Communications sent by post/courier, fax, electronic mail, text, chat and or any form of social media, etc.,
- Data stored and/or processed by servers, PC's, laptops, tablets, mobile devices, etc., and
- Data stored on any type of internal, external, or removable media or cloud based services.

Some Federal Policies to Be Familiar With...

(click the acronyms for additional info)

CIPA

Children's Internet Protection Act

COPPA

Children's Online Privacy Protection Act

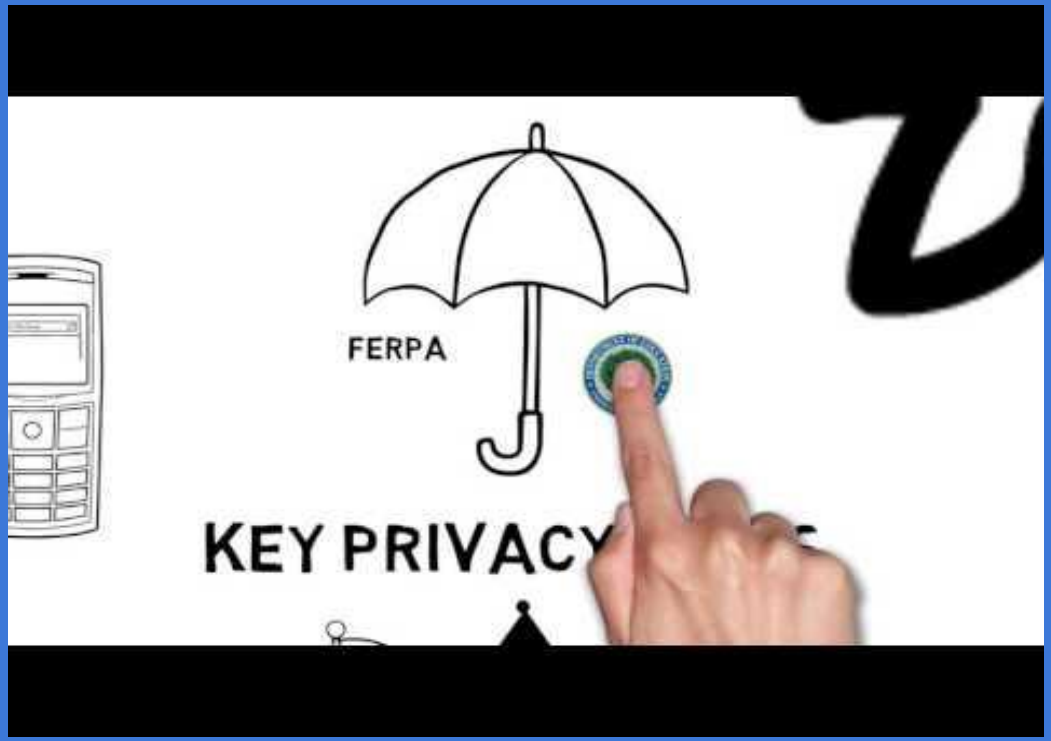
FERPA

Family Educational Rights and Privacy Act

HIPAA

Health Insurance Portability and Accountability Act

Watch this video on Student Privacy and FERPA
There is a quiz later, so watch carefully.



Definition of Directory Information

FERPA for School Officials- FAQ

FERPA regulations define directory information as information contained in an education record of a student that would NOT generally be considered harmful or an invasion of privacy if disclosed.

REMEMBER: FERPA Guidelines and the School System's POLICY are responsible for identifying this information. It is not open for debate or personal consideration.

KNOW what is included in the TCS Public Notice to parents.

KNOW which parents/guardians have opted out of disclosure of Directory Information.

KNOW the procedures for proper disclosure of Directory Information.

Directory information is part of the Education Record and includes personal information about a student.

By law, school systems may disclose directory information if it has given public notice to parents of students in attendance and eligible students in attendance concerning "directory information." (Responsibilities and Privileges pg. 34)

The Talladega County School System respects the privacy of students and does not share this information unless approved. Any large data export of information from iNow or other mass export MUST be approved by the DATA GOV committee and the vendor must have a signed MOA. Export/Import will be completed by the Technology Offices.

Mass Downloads and Sharing of Data with External Entities

*A sample MOA can be found in the Data Governance Policy

Mass Downloads to fulfill any request from an outside entity ***must be approved by the Data Governance Committee.***

When transferring PII to external entities such as software or application vendors, textbook companies, testing companies, or any other web based application, etc., the external entity must outline and ensure compliance to FERPA & any other laws or policies through a *Memorandum of Agreement (MOA).

So...What are YOUR responsibilities?

Review the Talladega County Schools System Data Governance Policy.

Note any procedural items pertaining to your job responsibilities.

Ask questions if you do not understand any part of the policy or need clarification.

When in doubt, err on the safe side.

Seek assistance from an expert or look over the PTAC online site before disclosing any data.

A little review…

Education Records are records that are directly related to a student and that are *maintained by an educational agency or institution* or a party acting for or on behalf of the agency or institution. These records include but are not limited to the following: grades, transcripts, class lists, student course schedules, health records (at the K-12 level), and student discipline files.

The information may not be recorded in any way, including, but not limited to, handwriting, print, computer media, videotape, audiotape, film, microfilm, microfiche, and e-mail.

?

What do you think?

A teacher or administrator writes a note/personal record on a pad of paper about a student's behavior in class (good or bad). Is this considered a student record, and would the student or parent have the right to gain access to that document under FERPA?

NO. Because this is a "sole possession" document (whether on paper or electronically on the PC) and NOT ***maintained by an educational agency or institution***, it does not fall under the definition of a student record. Therefore, a student or parent cannot use FERPA law to force a school system to produce that document. BUT... you still cannot leave that kind of information lying around!

?

What do you think?

Two teachers exchange e-mails about the performance of a common student. Could the parents/guardians ask to see this legally under FERPA?

YES. Such a document can be considered an educational record because it is maintained by the school system.

?

What do you think?

TCBOE designates name, address, telephone listing, email address, and honors and awards received as directory information. A non-profit organization that has programs for special needs children asks the school for directory information on students who have a certain disability. Can the names and contact information for these students be disclosed to the organization as directory information?

NO. Because TCBOE does not include "Student Disability" in the TCBOE Public Notice to parents. This type of student education record could generally be considered harmful or an invasion of privacy if disclosed.

?

What do you think?

A student creates and posts a blog, forum, etc. to fulfill a class assignment. Could this post ever be considered an educational record?

MAYBE. The opinion on this is vague. By having students post blogs, the teacher risks inadvertently asking students to reveal their class schedules and PII data that is protected under FERPA, so it should not be part of a public post. A simple solution in this case is for the teacher to give students a lesson on how to make their posts private or to make sure they clearly understand what they can or cannot post publically.

?

What do you think?

A teacher, coach, band director, sponsor, etc and a student exchange text messages. Is this protected under FERPA?

NO. If the texts are not maintained by the school system, they cannot be declared an educational record. *However, you should always be careful about texting students* unless it is a program that keeps your phone number private and the student's phone number private such as *Remind*. *Individual texts between a student and a staff member are highly discouraged.* These messages can sometimes be viewed as inappropriate communications between staff and students.

?

What do you think?

A student's health or safety is in question and 911 is called. Can we release information about the student to the EMT?

IF there is an *articulable and significant* threat to the health or safety of a student or other individuals, school officials may disclose PII to any person whose knowledge of the information is necessary to protect the health or safety of the student or other individuals.

This provision is for Emergencies only and cannot be used for disclosures on a routine, non-emergency basis, such as the routine sharing of non-directory information on students with the local police department (which is not allowed).

?

What do you think?

We use several 3rd party vendors to publish yearbooks, take school pictures, etc. If these vendors need the names and addresses of students, AND this is listed as Directory Information by the school district, can this information be provided to the vendor?

NO. YES. MAYBE. Even though the information the vendor requests is listed in the Directory Information, the vendor is performing a function under the "school official" exception...the vendor still must sign an MOA stating the terms and conditions which ensure they are compliant with FERPA. (Security of data, destruction of data, sharing data with marketers)

?

What do you think?

Is it permissible under FERPA to list the names of students who have overdue library books or other items by a library door, over the intercom, through a website, email, etc?

NO, nor can you post lists whereby students or parents owe money for any activity, etc.

?

What do you think?

Under FERPA, may a school nurse share medical information about students with other teachers and school administrators?

YES. At the elementary/secondary level, any records that a school nurse or health center maintains that are directly related to a student are considered "education records" subject to FERPA – not the HIPAA Privacy Rule. A school nurse may share information on students with other school officials if these school officials have a *legitimate educational interest* in the records.

ADDITIONAL Federal Laws & FERPA and Online Educational Services

There is a quiz later, so watch carefully.

What is an Online Educational Service?

1. Computer software, mobile applications (apps), or web-based tools that are…
2. Provided by a third-party to a school or district which are…
3. Accessed via the Internet by students and/or parents AND…
4. Used as part of a school activity.

Is it allowable under FERPA to share PII with Online Providers?

YES. But these are the requirements:

1. **Parental consent for the disclosure, OR…**

2. **Disclosure under one of FERPA's exceptions to the consent requirement, such as…**

1. **Directory Information (but remember, parents can "opt out"), OR…**

1. **School Official Exception...Oh, but wait!!! (next slide)**

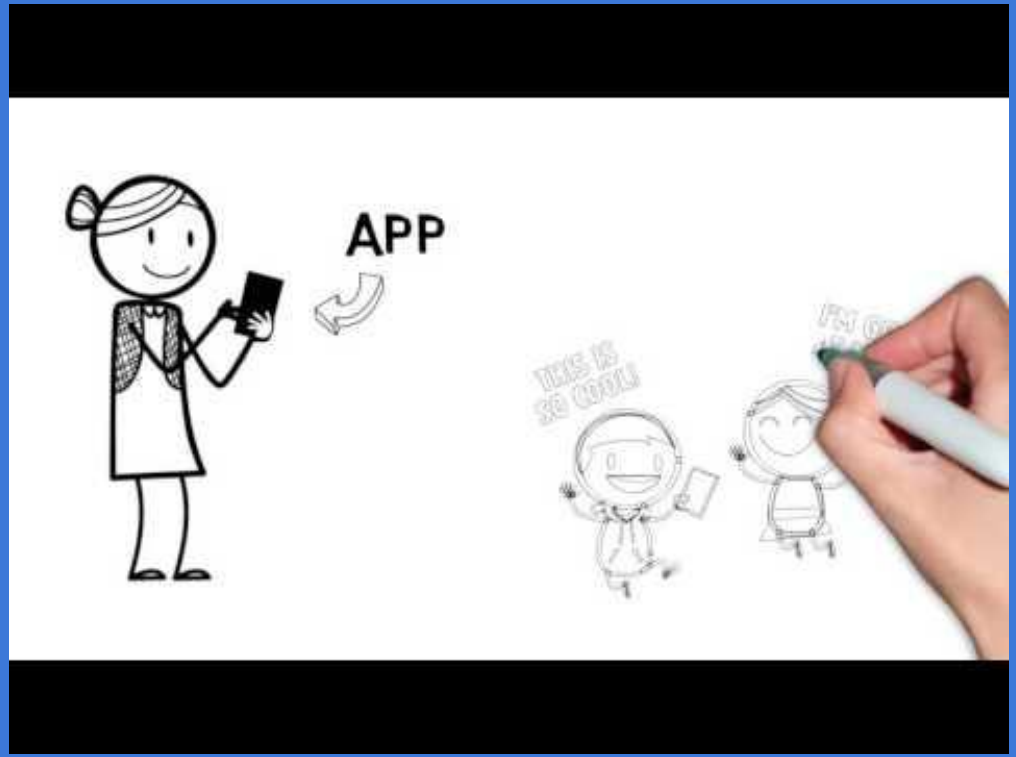
Using the "School Official Exception" to Share PII

DO NOT FORGET THAT SHARING PII WITH AN ONLINE SERVICE PROVIDER UNDER THE "SCHOOL OFFICIAL EXCEPTION" REQUIRES:

1. Annual FERPA Notice (Responsibilities & Privileges)
2. Local School Officials must maintain direct control over this data exchange
3. Use of PII only for authorized purposes
4. Limitations on redisclosure from the Online Service Provider to other entities

SO… this type of control must be guaranteed through a Memorandum of Agreement (MOA). The Data Governance Committee would be involved.

Watch this video on PII, COPPA, and Online Service Providers
There is a quiz later, so watch carefully.



COPPA

Children's Online Privacy and Protection Act (COPPA)
Applies to commercial Websites and online services directed to children under age 13, and those Websites and services who have knowledge that they have collected personal information from children.

Administered by the Federal Trade Commission
See the link below for more information.

http://www.business.ftc.gov/privacy-and-security/childrens-privacy for more information

Best Practices

Protecting Student Privacy and COPPA

Be aware of which online educational services are currently being used in your district

Have policies and procedures to evaluate and approve proposed educational services

When possible, use a written contract or legal agreement

Be transparent with parents and students

Remember the FERPA's requirements for schools and districts disclosing PII under the school official exception…

-Direct control
-Consistency with annual FERPA notification provisions
-Authorized use
-Limits on redisclosure

These services may also introduce security vulnerabilities into your school networks

The use of "freemium" services are highly discouraged.

Click-Wrap Agreements: Don't Do It!!!

When vendors, contractors, and other service providers rely on a Terms of Service (TOS) agreement that is not negotiated.

Usually offered in the form of an "I agree" check-box.

These agreements are referred to as "click-wrap" agreements, and can operate as a provider's legally-binding contract.

Click-Wrap Agreements!

Click-Wrap agreements could potentially lead to a violation of the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), or other laws, as well as privacy best practices.

The best way to handle a “click-wrap” agreement is to allow someone in the District Technology Offices to review it. If you “click” then YOU AGREE!

Online Apps/Sites/ Tools

When using an online app/site/tool, it is ESSENTIAL that the Terms of Service (TOS) be reviewed thoroughly.

The language in a TOS should be clear that the data collected cannot be used to advertise or market to students.

The amount of data collected by the provider should be limited to only what is necessary to fulfill the obligations of its agreement with the school or district.

BEST PRACTICE "Freemium" Apps/Sites/ Tools

Consult the Technology Offices to determine if the App has been approved for use in the district or poses any significant risk to the disclosure of student PII.

So…What Else Should You Know?

<u>Keep your log-in information and access to data private and protected.</u>

Do not keep student PII downloaded to your laptop or other mobile device unless the data is encrypted. *BEST PRACTICE - Do not store educational records/PII on devices that leave secure locations on campus.*

Never share your device with anyone when you are signed in, or data is accessible. *BEST PRACTICE - Do not share your device.*

Never discuss student PII in public places.

Who Can Access Data/PII in TCBOE Systems?

Access will be granted on a "need to know" basis and must be authorized by the Superintendent, Principal, immediate supervisor, or Data Governance Committee with the assistance of the Technology Coordinator/Data Governance Officer. On a case-by-case basis, permissions may be added to those already held by individual users in the student management system, again on a need-to-know basis and only in order to fulfill specific job responsibilities.

Security of Data Transmission

Data encryption should be utilized during data transmission over communications networks to minimize against unauthorized access.

Note: Emails exchanged within the tcboe.org and tcboe.net domains are encrypted, however, emails to and from outside entities have no guarantee of encryption protocols.

Best Practices for Email

- Always use your assigned tcboe.org email to communicate with students, parents, community members, vendors, educational entities, etc.

- Do NOT send PII through email or email attachments. Best practice is to share information through secure transfer portals or **direct sharing** (not through link creation, etc) within Google Drive.

- When composing emails, use care to refrain from using compulsive or unprofessional communications.

Legal Considerations of Email

- Any email exchanged by school system employees about individual students is public record.
- Any email pertaining to a particular student is discoverable in a due process situation or other legal action.
- The nature of email lends itself to impulsive, overly informal, and sometimes unprofessional communication.

Legal Considerations of Email

- ALL email (received, sent, and deleted) within the Google Apps for Education Suite is stored within Google Vault for “e-discovery” purposes for a period of EIGHT years.

Data Stored Remotely

Responsibilities of Data that is stored on a device, drive, or other method, including hard-copy:

Confidential data or PII that is stored or accessed remotely must maintain the same level of protection as data on the TCBOE network or approved cloud servers.

Users must never leave devices logged in, unattended, or open to unauthorized use.

No PII, Confidential and/or Internal Information should be stored on a device itself such as a hard drive, mobile device of any kind, or external storage device that is not located within a secure area AND that is not protected by a PASSWORD.

No technological systems that may contain confidential information or PII should be disposed of or moved without adhering to the appropriate Purchasing and Disposal of Electronic Equipment procedures.

Downloading and Printing Confidential Data

PII and Confidential Information must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise.

PII that is downloaded for educational purposes should be de-identified before use, whenever possible.

Email Questions to:

Dr. Brooke Morgan
Coordinator of Innovative Learning
brookemorgan@tcboe.org