



# Best Practices on Transparency in Using Student Information

Utah Privacy Conference  
November 6-7, 2018

**Ross Lemke**  
**Director**

Privacy Technical Assistance Center

United States Department of Education  
Privacy Technical Assistance Center

ADA Compliant December 2018

# A little exercise

- Using your phone or your laptop go to your district website
  - Search for "Privacy"
  - Search for "FERPA"
- What did you find?

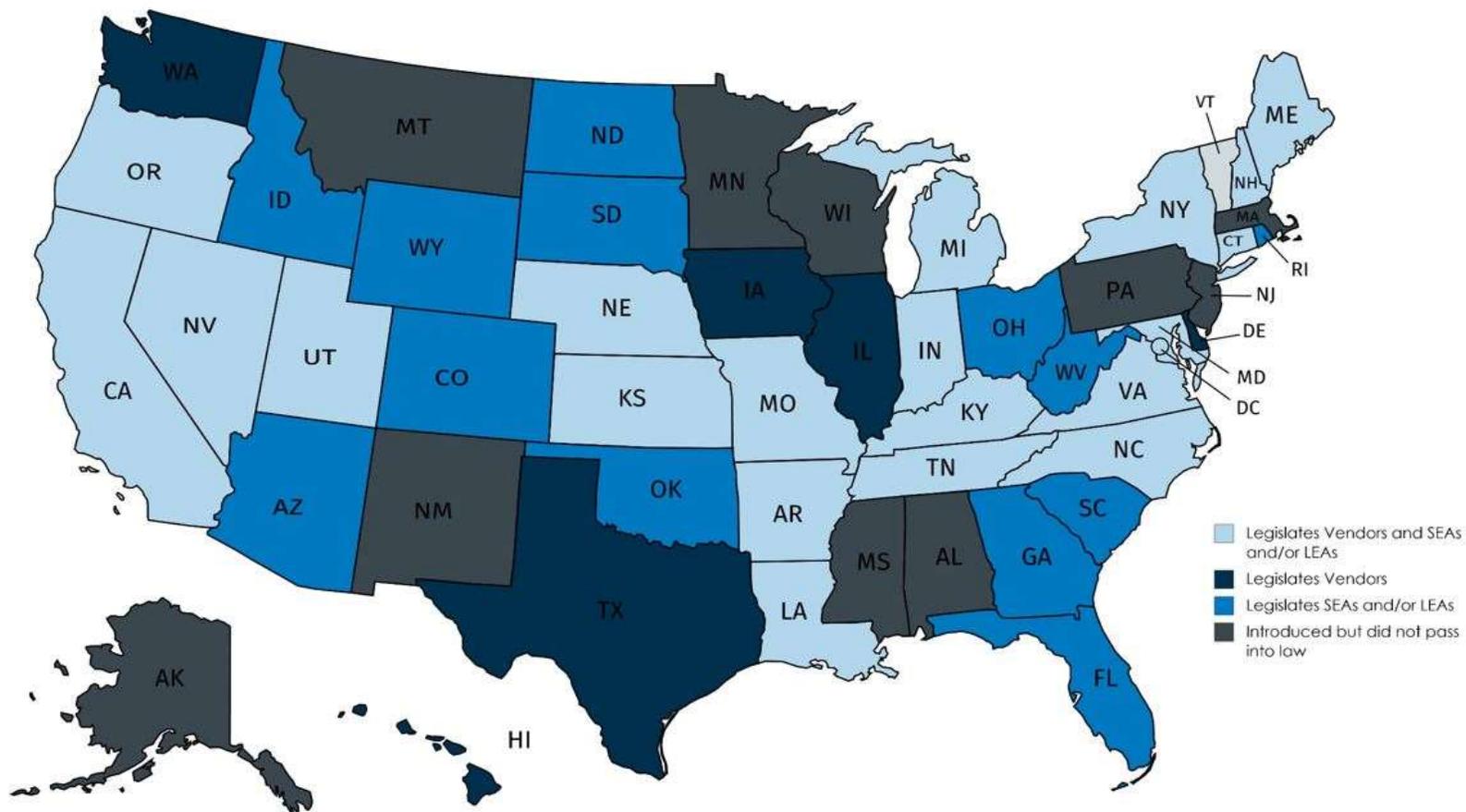


# Why Transparency?

- Rise in public discourse on data and student privacy.
- Rise in misinformation and confusion about the issues.
- State-level legislative action to restrict data collection, use, and sharing.

*In the absence of information, people will just assume the worst.*

# 40 States Have Passed 125 Laws Since 2013



<https://ferpasherpa.org/state-laws/>

Created with mapchart.net ©



# Why is Transparency Important?

- Parents expect openness and transparency from schools and districts about their data practices.
- Transparency allows a parent to evaluate if the protection of their child's personal information meets their expectations.
- Schools and districts should take a proactive approach in communicating with parents.
- The Department considers transparency in privacy practices of upmost importance to school districts



# Transparency – What is Required?

- FERPA requires certain information be provided to parents including:
  - Annual notification listing rights under FERPA including:
    - Right to inspect and review their education records.
    - Procedure for exercising that right.
    - Criteria for what constitutes a “School Official” and “Legitimate Educational Interest”.
  - Directory Information Policy including
    - Types of information designated as directory information.
    - Opt out provisions.
- PPRA requires districts notify parents of their rights annually.



# Best Practice Recommendations for Improving Transparency

Beyond Federal Privacy Law, the Department recommends best practices for improving transparency.

These recommendations can be divided into three main categories:

1. What information to communicate to parents.
2. How to convey that information.
3. How to respond to parent inquiries about student data policies and practices.



# Recommendations on What to Communicate to Parents

- As a best practice parents should be provided with the following information about your school's or district's data and privacy practices:



# Recommendations on What to Communicate to Parents (cont'd)

- What information are you collecting about students and why are you collecting this information?

**REMEMBER:** The first step in protecting sensitive information is knowing what information you have. If you cannot provide a good reason for why you are collecting a particular data element, you may want to reconsider collecting it.



# Recommendations on What to Communicate to Parents (cont'd)

- Why are you collecting this information?

**REMEMBER:** The volume of information being collected by a district as part of its day to day operations can be daunting. Consider providing rationale for why the data is being collected, whether it is to provide essential school services, improve instruction or to comply with federal law.



# Recommendations on What to Communicate to Parents (cont'd)

- How is the information protected?
  - Explain your IT security and data protection policies
  - Describe your policies governing the use of student data.
  - Explain your data retention policies
  - If you publish aggregate data, explain the privacy protections to protect against disclosure of student's PII in small cells.

**REMEMBER:** It is important to regularly train your faculty and staff on these IT and data protection policies.



# Recommendations on What to Communicate to Parents (cont'd)

- Do you share any personal information with third parties? If so, with whom, and for what purpose(s)?
  - Consider posting contracts online.
  - Provide a list of apps that are approved for the classroom.

**REMEMBER:** Let parents know the reasons you are sharing student data with a third party and explain the legal, contractual, and policy protections in place to safeguard the data.



# Recommendations on What to Communicate to Parents (cont'd)

- If you share student information with external researchers.
  - show parents the research findings.
  - identify if you made any changes to curriculum, policies, or programs as a result.



## Recommendations on What to Communicate to Parents (cont'd)

- Do you talk to parents about safe online behaviors?



- Who should parents contact if they have questions about your data practices?

**REMEMBER:** Posting information on a website is not enough – ask for constructive feedback from parents and students to ensure that the policies and practices are truly transparent

# Recommendations on How to Communicate about Data Practices

- When communicating with parents about the school's or district's data practices, consider the following best practices to improve accessibility and clarity of the messages...



# Recommendations on How to Communicate about Data Practices

- Use your website as part of a multi-layered approach to communication.
  - ✓ Match the sophistication of the message to the medium.
  - ✓ Post FERPA and PPRA notices on your website as a reference.



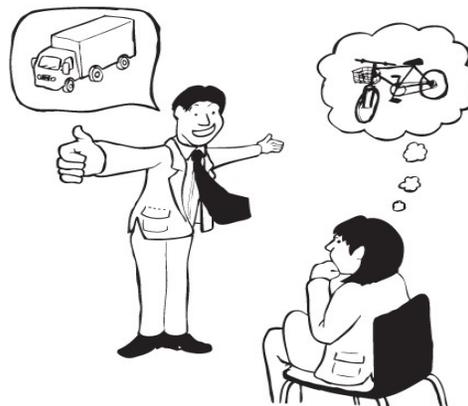
## Recommendations on How to Communicate about Data Practices

- Make your website user-friendly, searchable, and easy to navigate.
  - ✓ Consolidate information about data practices and privacy protections.
  - ✓ Clearly label the data practices/student privacy section and ensure that users can quickly navigate to it from the homepage with just one or two mouse clicks.
  - ✓ Add a “Search” tool to your website.



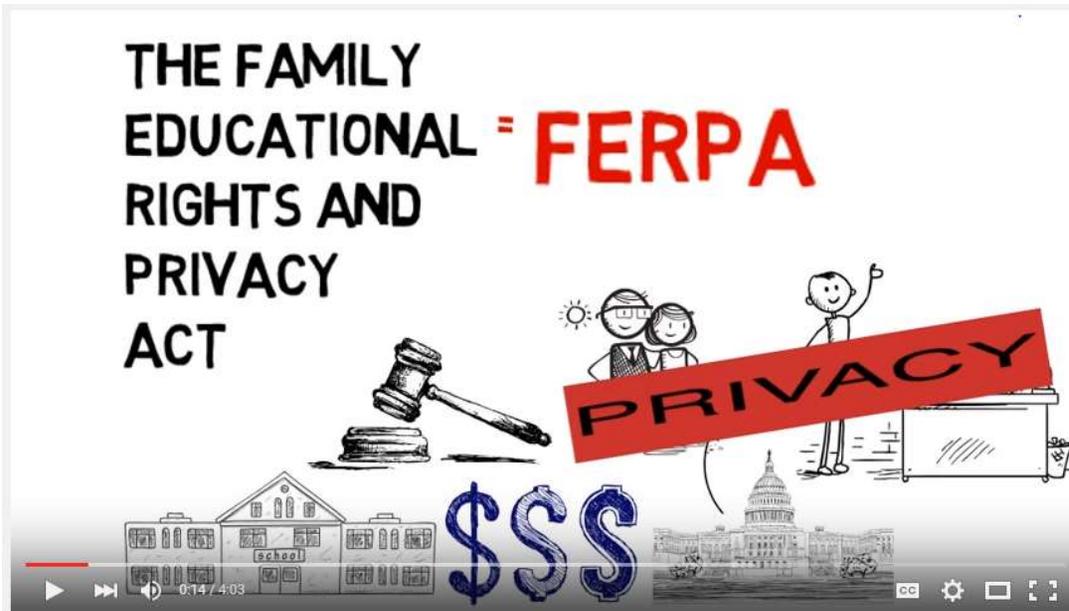
# Recommendations on How to Communicate about Data Practices

- Be clear and consistent.
  - ✓ Use plain language whenever possible.
  - ✓ Provide examples to illustrate complex concepts or ideas.
  - ✓ Include a glossary.
  - ✓ Make sure that your website's data practices section is accessible to persons with disabilities.
  - ✓ Translate information on your website into other languages commonly spoken in your community.
  - ✓ Maintain consistency across communication mediums.



# Recommendations on How to Communicate about Data Practices

- Leverage existing resources.
  - ✓ Link to relevant resources outside your district.
  - ✓ Pool resources with other districts – Don't feel you need to invent everything yourself



# Recommendations on How to Communicate about Data Practices

- Have members of the community regularly review your website for useability, comprehension, and completeness.
  - ✓ Follow up with parents and students to ensure your site is user-friendly.
  - ✓ Solicit feedback from parents and students on recommended improvements to your website



# Where do I start?

- [PTAC Guidance Videos](#)
- [Transparency Best Practices](#)

HOW TO USE YOUR DISTRICT'S WEBSITE TO COMMUNICATE WITH PARENTS ABOUT DATA USE AND SECURITY

Privacy Technical Assistance Center  
U.S. Department of Education

0:05 / 2:15

PARENT COMMUNICATION STRATEGY

- USE CLEAR, SIMPLE LANGUAGE
- PROVIDE EXAMPLES
- INCLUDE GLOSSARY
- MAKE IT EASY FOR PARENTS TO FIND INFORMATION
  - CONSOLIDATE INFORMATION
  - PROVIDE CLEARLY LABELED LINK FROM THE HOME PAGE

1:22 / 2:15



Let's look at some examples...



# Fairfax County Public Schools

## Privacy Information Security Strategies and Practices

FCPS provides extensive systems resources that manage student information in direct support of the learning process and the administration of instruction. Some major systems that maintain student information include FCPS 24-7 Learning (Blackboard), the student information systems (SIS, SASI, and SEA-STARs), the data warehouse (EDSL), and eCART. We believe in protecting the confidentiality, integrity, and availability of the student information in accordance with the value and risk of the data.

There is a trade-off between access to student information and the risk of unauthorized use—the more accessible student information is to more users, the greater the risk of unauthorized disclosure. To mitigate this risk, FCPS implements a comprehensive information security program to protect student information encompassing physical, network, systems, procedural, and user security ([FCPS Information Security Policy—Regulation 6225](#)):

## Rights and Responsibilities

All FCPS stakeholders have the responsibility to use FCPS digital resources in accordance with the law, FCPS regulations, and FCPS best practices guidelines and have rights and responsibilities as follows:

- Privacy (P).
- Safety (SA).
- Security (SE).
- Use and access to information (U).



# Denver Public Schools

## Student Data Privacy



STAFF: REQUIRED VIDEO & GUIDANCE

PUBLIC TRANSPARENCY

LEGAL

Required Video

+

Using Online Tools – For Teachers

+

Using Online Tools – For Principals

+

Rules for Storing and Sharing Student Data – For All

+

Social Media Usage

+

### Links

FERPA-Approved App List

Board Policy JRA/JRC Student

Records/Release of Information on  
Students

Standard Terms of Use to be Completed  
by Vendors Serving as School Officials  
[docx]

Archives: Parent Consent Forms

CEPI Home Contact CEPI MI.gov

# Center for Educational Performance and Information

Search

- About CEPI
- CEPI Applications
- Calendar
- Get Data
- e-Transcript
- Nonpublic Schools
- Institutions of Higher Education
- MI School Data
- Michigan Longitudinal Data System
- Help and Support
- MI School Data

## CEPI

### Pupil Privacy

Public Act 367 of 2016, Protection of Pupil Privacy, requires that the Michigan Department of Education (MDE) and the Center for Educational Performance and Information (CEPI) post on their websites a notice of the information collected for a pupil's education records, including an inventory of all pupil data elements and a description of each pupil data element. In addition, Section 1136(1)(d) specifies that CEPI and MDE will not disclose any information concerning a pupil that is collected or created except in accordance with the established policy that details how they will protect and distribute student data.

[The Michigan Student Data System \(MSDS\) Data Use Matrix](#) is an Excel document showing how the student data CEPI collects in the MSDS support federal and state reporting requirements. The matrix also shows whether a field is required, optional, or required only if relevant (E.g., districts only report Title I eligibility for students who are Title I eligible.) For additional information, please see [How Your Data Are Used](#).

CEPI is committed to protecting confidential education records, and to transparency when it comes to data collection, storage and disclosure. Our data security protocols follow strict State of Michigan standards and best practices. Our rigorous privacy policies and procedures meet or exceed data sharing guidelines of the Family Educational Rights and Privacy Act (FERPA).

For more information on how CEPI safeguards the data it collects, please see [How CEPI Protects Education Data](#). For information on how MDE protects the data they collect, see [MDE's Pupil Privacy page](#).



# New York State Department of Education

NYSED Education Areas Standards & Curriculum Assessments Certification & Licensing School Business Data & Reporting

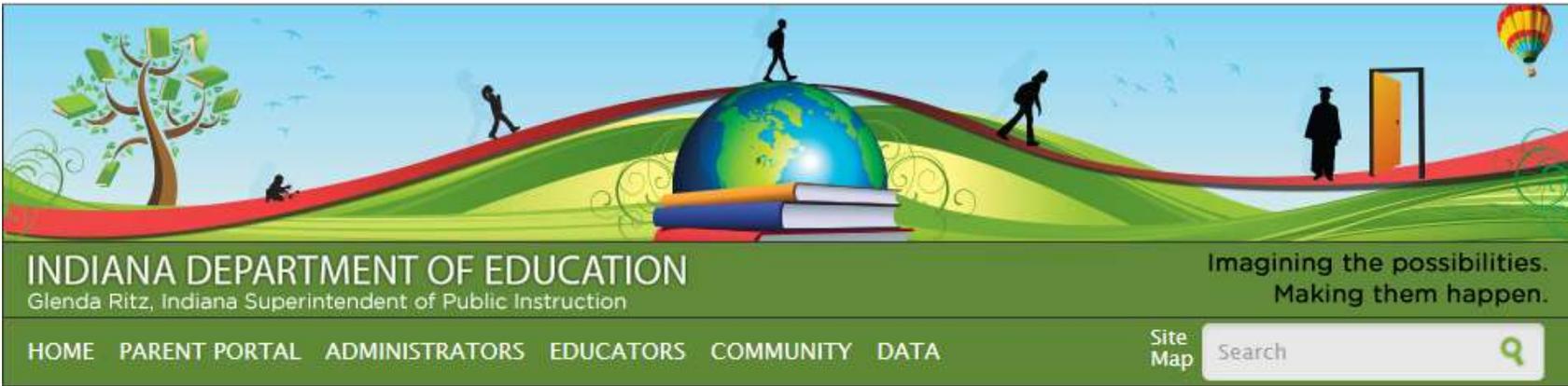
Student Data Privacy

- Student Data Privacy: Education Law
- Student Data Privacy Bill of Rights (Parents' Bill of Rights)
- Report an Improper Disclosure
- Website Feedback
- Contact Information
- Frequently Asked Questions

## Frequently Asked Questions About Student Data Privacy

- 1. Can companies that provide services to my school under contract (third party contractors) buy my information or use it for their marketing purposes?**  
No. Your personally identifiable information (PII) cannot be sold by a contractor or used for marketing purposes.
- 2. Must I be notified if there is an unauthorized disclosure of my personally identifiable information?**  
Yes. The school must notify the parent or eligible student of the unauthorized release of student data in the most expedient way possible and without unreasonable delay. This applies to cases of an unauthorized release of teacher or principal personally identifiable information data as well. Each





[Home](#) > [Accountability](#) > Data Collection

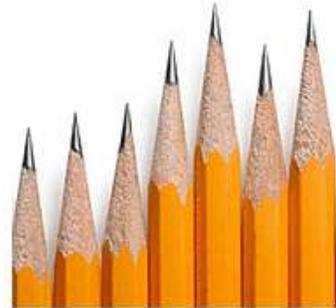
## Data Collection

Posted: Tue, 03/20/2012 – 9:30am Updated: Mon, 01/05/2015 – 2:58pm

Welcome to the Data Collection Home Page. Data collected on students, employees, and schools are used for state and federal reporting and collected via the [STN Application Center](#) or [DOE-Online](#) by the department. In the Data Collection and Reporting Community in [Learning Connection](#) you will find specific requirements, instructions and technical support for submitting data in a timely and accurate manner. The [Data Collection and Reporting Help](#) page will have direct links to data layouts and current postings.

### Areas to Explore

- [How The Data Are Used](#)
- [Why Data Are Collected](#)
- [Where Data Are Collected](#)
- [When The Data Are Collected](#)
- [How The Data Are Collected](#)



### Accountability

- A-F Accountability
- Data Collection
- Data Center

### January

				1	2	
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24





**VIRGINIA DEPARTMENT OF EDUCATION**

Home » Information Management

Search

**INFORMATION MANAGEMENT**

Longitudinal Data System

Data Quality

Data Collection

**Resources:**

- SSWS Login
- SSWS User Guide (PDF)
- The Calendar of Reports (PDF)
- Procedures for Data Collection & Reporting (PDF)
- Registering Students From Language Backgrounds Other Than English (PDF)
- Information Technology Security Policy Statement (PDF)

**You May Also Be Interested In:**

- Statistics & Reports
- OMEGA

**CONTACT US**

Information on this page is provided by the [Office of Educational Information Management](#).

**INFORMATION MANAGEMENT**

The effective use of accurate and detailed information on student achievement and other school-quality factors is central to Virginia's commitment to providing quality instruction for all students. VDOE uses information on achievement and school quality to shape policy decisions and help educators at all levels gather, analyze, and use data to improve teaching and learning – while protecting student privacy.



In addition, the Standards of Quality require the Board of Education and local school boards to adopt comprehensive, unified, long-range plans based on data collection, analysis of data, and how data are utilized to improve classroom instruction and student achievement.

**TIP: Finding your way around the site** – Use the menu to the right to navigate to the sub-sections of this topic, find related topics and access VDOE office and staff contact information.

**The Virginia Longitudinal Data System (VLDS)**

The Virginia Longitudinal Data System provides Virginia citizens, researchers, and policymakers with a single point of access to educational and workforce training data from multiple, independent sources while protecting the privacy of students.

What is VLDS? Learn about the Virginia



Vicki Luis Danny



**COLORADO**  
Department of Education

Site Index | CDE Offices | Staff Directory

Search

SchoolView | Data & Accountability | Programs & Supports | Teaching & Learning | Policy & Funding

**\*\* CDE will be closed on Monday, May 29 for the Memorial Day holiday. \*\***

Home

## Data Privacy and Security

### Announcement

CDE has updated our data dictionary to provide parents, districts, and others with easy to access and clear information on the Personally Identifiable Information (PII) CDE collects in our data system. The dictionary provides information on CDE's collections, the data elements within each collection, a description of each data element, and the state or local laws related to that collection. [Click here to be taken to the Data Dictionary.](#)

### Background

In this age of data-driven decision making, data is foundational to the success of the process. Whether discussing student-achievement, program monitoring, education funding, accountability or any other education-related conversation, data is at the center of the discussion. The Colorado Department of Education (CDE) is required by state and federal law to collect and store student and educator records.

CDE takes seriously its obligation to protect the privacy of data collected, used, shared and stored. These pages contain state and federal policies CDE adheres to, data privacy and security procedures, as well as guidance and resources for various stakeholders.

### Find it Now

- [Agreements and Contracts](#)
- [CDE's Major Data Collections](#)
- [CDE Policies and Procedures](#)
- [District and School Resources](#)
- [Federal and State Laws](#)

### Meeting Presentations

[View the presentation from CDE's Privacy Public Meeting on May 24, 2016](#) (PDF). As promised, CDE has provided answers to the questions asked during the public meeting. Those answers are on our new [Questions and Answers](#) page.

Below are the presentations from the PTAC-CDE Privacy training on May 25 and 26, 2016.

- [PTAC - Data Breach](#) (PDF)
- [PTAC - FERPA 101](#) (PDF)
- [PTAC - Terms of Service](#) (PDF)
- [PTAC - Transparency](#) (PDF)
- [CDE - New Colorado Data Privacy Law](#) (PDF)

### Keep Informed

Interested in receiving updates on CDE's work regarding data privacy and security? Subscribe to the CDE Data Privacy-Security email list.

[Subscribe](#)

Learn More

- [Additional Research & Reports](#)



## Remember this?

- Using your phone or your laptop go to your district website
  - Search for "Privacy"
  - Search for "FERPA"
- What did you find?



# Transparency (We are all among friends!!)

- Pretend you are a member of the public searching for information about data efforts in your Agency.
  - Is it easy to find your website?
  - Is there information on what data is being collected and why?
  - Can you find the information on data collection easily?
  - Is there a "search" feature on the site?



- Can you locate information on data privacy and transparency policies?
- Is the information presented in a clear, concise and consistent manner?
- Is there a glossary of terms available?
- Does the information address who has access to the data and for what purposes?
- Contact information - Is there an email address and/or phone number if the public/parents want more information on these data systems or their rights?



# Image Redacted

The screenshot shows a website for Salt Lake City School District and Provo City School District. The top navigation bar includes language options (English, Español, Tiếng Việt, Soomaali, More), a home icon, phone number (801-578-8599), and links for Employees and Login. Below this is a secondary navigation bar with links for Schools, Departments, Calendars, Directory, and Board, along with a search icon. The main content area is mostly obscured by a large black redaction box. To the right of the redaction, there are social media icons for Instagram, Twitter, and Facebook, and a search bar labeled "Search this web". Below the redaction, the text "LOYMENT" is visible. On the left side of the page, the Provo City School District logo is present, followed by a "NEWS" section and a breadcrumb trail: "Home / Student Services / Family Education Rights Privacy". The main heading "Family Education Rights and Privacy Act (FERPA)" is partially visible. Below the heading, there is a paragraph of text: "The Family Education Rights and Privacy Act (FERPA) gives parents and eligible students the right to inspect education records, the right to request amendments to records, the right to request that non-public personal identifiable information be removed from records, and the right to file a complaint with the Department of Education if a complete disclosure statement is not provided. For more information, please contact your school administrator." Below this text is a list of links with document icons: "Notification of Rights under FERPA", "Notice for Directory Information", "Aviso de Derechos bajo FERPA (Letra de Derechos)", and "Aviso de Información de Directorio".



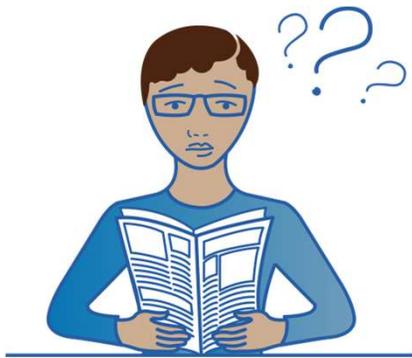
# Recommendations for Responding to Parent Inquiries

- Sometimes parents or students will contact you wanting additional information
- The Department of Education encourages schools and districts to handle parental and student inquiries about data privacy in a responsive and meaningful fashion
- The best practices include...



# Recommendations for Responding to Parent Inquiries (cont'd)

- Keep the lines of communication open
- Review parental inquiries, concerns, and suggestions in a thoughtful and careful manner
- Respond to parental or student inquiries in a timely manner
- Periodically review old inquiries and resolutions to evaluate your communication and transparency efforts



# Transparency Takeaways

- Reflect on the perspective of Agency and what qualities you want your stakeholders to associate with it.
- Consider how you might be able to improve your district's transparency.
- Address what are the benefits of your data system and the information obtained.
- Contemplate producing reports and FAQs to address data transparency questions/concerns.
- Update information as you receive feedback and requests from stakeholders for continuous improvement.



# Highlight your Successes

- Show the value of the data that you are entrusted with
- If you have made a meaningful change to how you educate your children as a result of data – Tell the World



# Department Strategic Objective 3

Strengthen the quality, accessibility and use of education data through better management, increased privacy protections and **transparency**.

- **Strategic Objective 3.2**

- Improve privacy protections for, and **transparency of**, education data both at the Department
  - Review a representative sample of Local Educational Agency websites for the transparency of their data practices and compliance with federal privacy laws when contracting with third party vendors.



# Why ED is undertaking this project

- Fordham University 2013 Report
  - ✓ LEA's doing a poor job projecting privacy (ed tech)
  - ✓ Districts weren't properly informing parents
  - ✓ Contracts had weak, non-privacy/security centric controls

However, there were some methodological issues from the conclusions drawn based on sampling strategy employed.



# PTAC's Approach to Website Transparency Review

- Develop appropriate, representative sampling strategy representative of the nation's school districts
- Devise a survey and audit checklist to assess legal compliance and best practice approaches employed by districts via their website
- Develop a series of public reports with detailed summaries of findings and best practices for districts to improve student privacy



# Objectives

- ✓ Inform ED/OCPO staff of the current state of privacy and transparency relating to data practices across the country
  - ✓ Better ED prioritization of guidance and TA
- ✓ Provide concrete feedback on privacy compliance and transparency best practices to each LEA in the sample to help LEA's improve data privacy practices
- ✓ Yearly public reports that allow SEA/LEA officials to address privacy and transparency within their jurisdictions
  - ✓ No LEA's will be identified in our public reports



# Sample Criteria

- Availability of required notices (FERPA, DI)
- Content of required notices (readability, specificity, etc.)
- Data page on LEA website
- Legal compliance with 3<sup>rd</sup> party contracting



# Draft Timeline

- Summer 2018 – Sampling criteria reviewed and approved by NCES/ED
- September 2018 – Survey Finalized
- September 2019 – 35% of website reviews completed, individualized reports sent to reviewed LEAs
- September 2019 – 2022 – Remaining LEA websites reviewed and individualized reports in corresponding years sent to LEAs which were reviewed
- Late Fall 2022 – Final Report on review project completed



# Where do I start?

- [PTAC Guidance Videos](#)
- [Transparency Best Practices](#)

HOW TO USE YOUR DISTRICT'S WEBSITE TO COMMUNICATE WITH PARENTS ABOUT DATA USE AND SECURITY

Privacy Technical Assistance Center  
U.S. Department of Education

0:05 / 2:15

PARENT COMMUNICATION STRATEGY

- USE CLEAR, SIMPLE LANGUAGE
- PROVIDE EXAMPLES
- INCLUDE GLOSSARY
- MAKE IT EASY FOR PARENTS TO FIND INFORMATION
  - CONSOLIDATE INFORMATION
  - PROVIDE CLEARLY LABELED LINK FROM THE HOME PAGE

1:22 / 2:15

# CONTACT INFORMATION

United States Department of Education,  
Privacy Technical Assistance Center



(855) 249-3072  
(202) 260-3887



[privacyTA@ed.gov](mailto:privacyTA@ed.gov)



<https://studentprivacy.ed.gov>



(855) 249-3073

