

# Using Educational Technology in the Classroom: AKA It's 10:00, Do You Know Where Your Student Data Are?

May 7, 2019

**Ross Lemke**
Privacy Technical Assistance Center

United States Department of Education
Privacy Technical Assistance Center

1

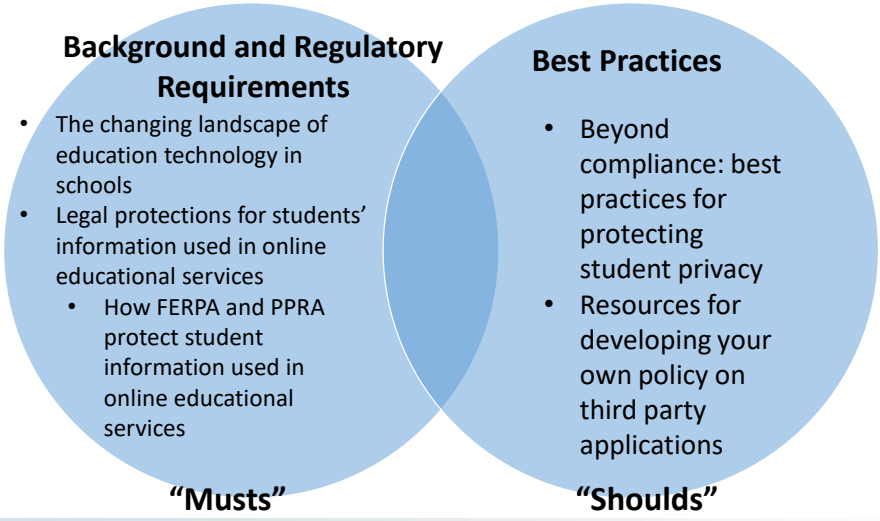
## Should you be here?

- Does your district use Educational Technology in the classroom?
- Do you know every app your teachers are using?
- Do you know what student data is getting put into those apps?



2

# Summary of Today's Discussion






3

# Online Educational Services

Today's guidance relates to the subset of education services that are:

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



**This guidance does not cover online services or social media used in a personal capacity, nor does it apply to services used by a school or district that are not accessed by parents or students.*



4

## The Challenge of Online Educational Services

- Schools and districts are increasingly contracting out school functions.
- We have new types of data, and much more of it!
- Many online services do not utilize the traditional 2-party written contractual business model.
- Increasing concern about the commercialization of personal information and behavioral marketing.
- We need to use that data effectively and appropriately, and still protect students' privacy.







## PTAC's Favorite Line from EDTech Vendors

- "Our Software is FERPA Compliant. We're School Officials."





## Things that don't Exist

- Unicorns
- Dragons
- Official Department

of Education FERPA

seal of approval







## How does the vendor get the data?

- Under FERPA, to share data with a vendor it has to happen under two ways:
  - Consent
    - Consent must be signed and dated and must:
      - Specify the records that may be disclosed
      - State purpose of disclosure; and
      - Identify party or class of parties to whom disclosure may be made
  - One of the exceptions under FERPA:
    - Directory Information Exception
    - School Official Exception





## Directory Information

- Information in a student's education records that would not generally be considered harmful or an invasion of privacy if disclosed.
- This may include: Name, address, phone number, grade, photograph….
- Each district determines their own directory policy which includes an opt out provision.
- Some districts use a limited directory information policy that restricts who can receive directory data.







## Problems with Directory Information and Consent

- Under Directory Information, parents and eligible students can opt out which may affect your ability to get a complete data set.
- Using consent, you may not get consent from everyone.





## School Official Exception

- Schools may disclose PII from education records without consent if the disclosure is to other school officials within the school, including teachers, whom the school has determined to have legitimate educational interest.
- Schools may outsource institutional services or functions that involve the disclosure of education records to contractors, consultants, volunteers, or other third parties provided certain conditions are met.







## Conditions for Outsourcing

- Performs an institutional service or function for which the agency or institution would otherwise use its employees;
- Is under the direct control of the agency or institution with respect to the use and maintenance of education records;
- PII from education records may be used only for the purposes for which the disclosure was made, and may not be redisclosed without the authorization of the educational agency or institution and in compliance with FERPA;
- Meets the criteria specified in the school, LEA, or institution's annual notification of FERPA rights for being a school official with a legitimate educational interest in the education records.





## Annual Notice

- Each school or district has an annual notification of FERPA rights which includes criteria for determining who constitutes a school official and what constitutes a legitimate educational interest.
- The definition of a school official may vary from one district to another.







## Question

Under FERPA, are providers limited in what they can do with the student information they collect or receive?





## Are providers limited in what they can do with the student information they collect or receive?

If PII is disclosed under the Directory Information exception:

- No limitations other than what the school/district includes in their agreement with the provider.

If PII is disclosed under the School Official exception:

- PII from education records may only be used for the specific purpose for which it was disclosed.
- TPPs may not sell or share the PII, or use it for any other purpose except as directed by the school/district and as permitted by FERPA.

*When personal information is collected from a student, the PPRA may also apply!*

- *PPRA places some limitations on the use of personal information collected from students for marketing.*







## What about metadata?

"Metadata" are pieces of information that provide meaning and context to other data being collected, for example:

- Activity date and time
- Number of attempts
- How long the mouse hovered before clicking an answer

Metadata that have been stripped of all direct and indirect identifiers are not protected under FERPA (note: school name and other geographic information are often indirect identifying information in student data).

Properly de-identified metadata may be used by providers for other purposes (unless prohibited by their agreement with the school/district).





## FERPA is not the only game in town when it comes to student privacy

- Other Federal Laws
  - PPRA
  - COPPA
- State and Local Laws







## Protection of Pupil Rights Amendment (PPRA)

- Amended in 2001 with No Child Left Behind Act
- Mostly known for its provisions dealing with surveys in K-12
- Includes limitations on using personal information collected from students for marketing
- May require parental notification and opportunity to opt out
- May require the Development of policies in conjunction with parents
- However … a significant exception for "educational products or services"





# COPPA

- Children's Online Privacy and Protection Act (COPPA)
  - Applies to commercial Web sites and online services directed to children under age 13, and those Web sites and services with actual knowledge that they have collected personal information from children
  - Administered by the Federal Trade Commission
  - See http://www.business.ftc.gov/privacy-and-security/childrens-privacy for more information







# COPPA

- Statute enacted in 1998, Rule revised in 2012
- Goals are to:
  - Allow parents to make informed choices about when and how children's personal information is collected, used, and disclosed online.
  - Enable parents to monitor their children's interactions and help protect them from the risks of inappropriate online disclosures.
- Operators of commercial websites, apps, and online services must provide NOTICE and obtain parental CONSENT before collecting personal information from children under age 13.





## COPPA Applies To:

- Child-directed sites and services.
- General audience sites with actual knowledge they're collecting personal information from kids under 13.
- Third parties with actual knowledge they're collecting personal information directly from users of a service directed to children.







## "Collects or collection"

- Requesting, prompting, or encouraging that children submit personal information online, even when optional.
- Enabling children to make the information public, *e.g.,* in a chat room or profile.
- Passive tracking linked to personal information.





## Under COPPA, operators must:

- Notice
  - Post a privacy policy and links to the policy wherever personal information is collected.
  - Give parents direct notice of its information practices.
- Consent
  - With certain exceptions, obtain verifiable parental consent before collecting information.







## COPPA and Schools

- Can operators get consent from schools instead of parents to collect personal information from students?
  - Yes if for the use and benefit of the school and no other commercial purpose.
  - Teacher, school, district? Best practice is go through school or district.





# FTC Act Enforcement

- Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."
- Deception: a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances.
- Unfairness: practices that cause or are likely to cause substantial injury to consumers that are not outweighed by countervailing benefits to consumers or competition and are not reasonably avoidable by consumers.







# STUDENT PRIVACY PLEDGE

- More than 300 companies have signed on to the student privacy pledge, which makes clear that the school service providers will:
  - Not sell student information;
  - Not behaviorally target advertising
  - Use data for authorized education purposes only
  - Not change privacy policies without notice and choice
  - Enforce limits on data retention
  - Support parental access to, and correction of errors in, their children's information
  - Provide comprehensive security standards
  - Be transparent about collection and use of data





## About the Student Privacy Pledge

- The pledge is not administered by the Department of Education.
- It is **not** a FERPA seal of approval.
- It **is** an example of the EDTech industry trying to regulate itself.
- For companies signing on, failure to do so may be a deceptive trade practice under the FTC Act.







- If so, you may leave
- If not, you may want to stay





## Can individual teachers sign up for free (or "freemium") education services?

Here's a better question: Should individual teachers sign up for Free or "Freemium" services?







## Using free or "freemium" educational services

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

- Direct control
- Consistency with annual FERPA notice provisions
- Authorized use
- limits on re-disclosure

These services may also introduce security vulnerabilities into your school networks.






**It is a best practice to establish district/school level policies governing use of free/freemium services, and to train teachers and staff accordingly.**





## Question:

Should school or district staff be concerned if a TPP uses a "Click-Wrap" or Terms of Service agreement instead of a traditional contract?







## Answer: It Depends

- Click-wrap or Terms of Service (TOS) agreements are not prohibited.
- Nothing in FERPA says that staff cannot click that "Accept" button.
- However, there are some considerations… (like everything else we've discussed today)





## Click-Wrap Agreements

- These agreements are referred to as "click-wrap" agreements, and can operate as a provider's legally-binding contract.
- Once a user at your school or district clicks "I agree," the terms of this agreement will likely govern what information the provider may collect from or about students and with whom they may share it.







## Click-Wrap Agreements (cont'd)

- 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 onus is on the school or district to review the TOS to see if it is acceptable and complies with Federal and State law.
- The TPP has a click-wrap agreement to protect them, not necessarily you.





# Privacy-Related TOS Provisions

- The example provisions are intended to give you a general idea of what to expect when reviewing a TOS.
  - Please keep in mind that specific language will vary from TOS to TOS.
  - Language matters and just because the TOS says that the vendor can do something does not mean that FERPA permits it.







# Pie Mogul – The App

**Terms and Conditions**

I agree to the terms and conditions of Pie Mogul: The App.

| Cancel | Agree |
|---|---|







## What is Data?

"Data include all personally identifiable information (PII) and other non-public information. Data include, but are not limited to, student data, and user content."

"Data only include information provided by the user in the course of using this service."







## Data Collection

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.





# Data Use

"Data use" by a provider should be limited to the purposes outlined in the agreement with the school or district.

Beware of any provision that contains the phrase "without providing notice to users."

If the School Official Exception is in use remember:

Legitimate Education Interest







# Data Use

- Information gathered in an online educational service or mobile application could be used to create a profile on a student.
- That profile could then be used to direct advertising/marketing materials to students.
- The language in a TOS should be clear that the data collected cannot be used to advertise or market to students.
  - Targeted advertising/marketing could violate privacy laws.





## Data De-Identification

- Even stripped of identifiers, student data could still be identifiable (through demographic or contextual information collected by the app, or through information available elsewhere).
- It can be difficult (and arguably impossible) to completely de-identify data.







## Security Controls

- Student data need to be protected, and a provider's TOS should include provisions outlining strong policies safeguarding those data.
- Failure to provide adequate security could lead to a FERPA violation.





## Modification of Terms of Service

"Pie Mogul may modify the terms of this agreement at any time. Notice of these changes will be available on our website. Please visit the website periodically to become aware of these changes."

"Pie Mogul will provide notice and obtain consent from the school prior to any change in the way data is collected, used, or shared under the terms of this agreement."







## Access

- FERPA requires schools and districts to make education records accessible to parents.
- To fulfill FERPA requirements, providers need to make student data available upon request.
- As a best practice, data should be passed from the provider to the school/district.





## Rights and License in and to Data

- Schools/Districts should maintain ownership of student data.
  - Some TOS include provisions that would grant providers an exclusive and irrevocable license to student data.
    - This can be a cause for concern.
    - If a license is granted, it should be limited and only allow student data to be used for educational purposes as outlined in the agreement.









## What Now?

"This session makes you not want to use any third party programs."

## Technology is here to stay

- Education Technology can do some great things.
- As education professionals it is our responsibility to ensure that these tools are used appropriately.
- The first step in this is to develop a policy on the use of apps in the classroom.







## Don't be the "No" Person

- Educators want to use this technology.
- If they are told no, odds are they will do it anyways.
- By coming up with a policy and procedure you are able to ensure that the technology is used on your terms.





## Developing District Policy

- Every school or district should have a policy in place for reviewing agreements before the service or application is used in the classroom.
  - Schools/Districts should establish a review process and/or have a designated individual review TOS before its adoption.
  - The service or application should be inventoried, evaluated, and support the school's and district's broader mission and goals.
- Get leadership buy-in and support for the new policy.







## Policies and Procedures to Approve Educational Services

- Test and evaluate popular services to see if they are right for your district.
- Evaluate terms of service to ensure they are satisfactory.
- Consider developing a repository of "approved" apps.
- Training, Training, Training!





## Training Resources

- PTAC Training Video
- Upcoming PTAC Teacher Training Modules










## ~~Steal~~ Leverage the Work of your Peers

- Student Data Privacy Consortium: Searchable database of vetted applications
- California Education Technologies Professionals Association : Searchable database of vetted applications and vetted terms of service
  - *Note: The U.S. Department of Education cannot endorse these or any other organizations' resources. Districts should consult with their legal counsel to ensure compliance of classroom applications with federal, state, and local laws.*





## Best Practices for Protecting Student Privacy

- Maintain awareness of other relevant laws.
- 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.
- Consider that parental consent may be appropriate.







## Discussion Questions

- Do you have a policy in place for the acceptable use of apps and technology in your classrooms?
- Do you know all of the apps currently being used in your classroom?





## A little exercise

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







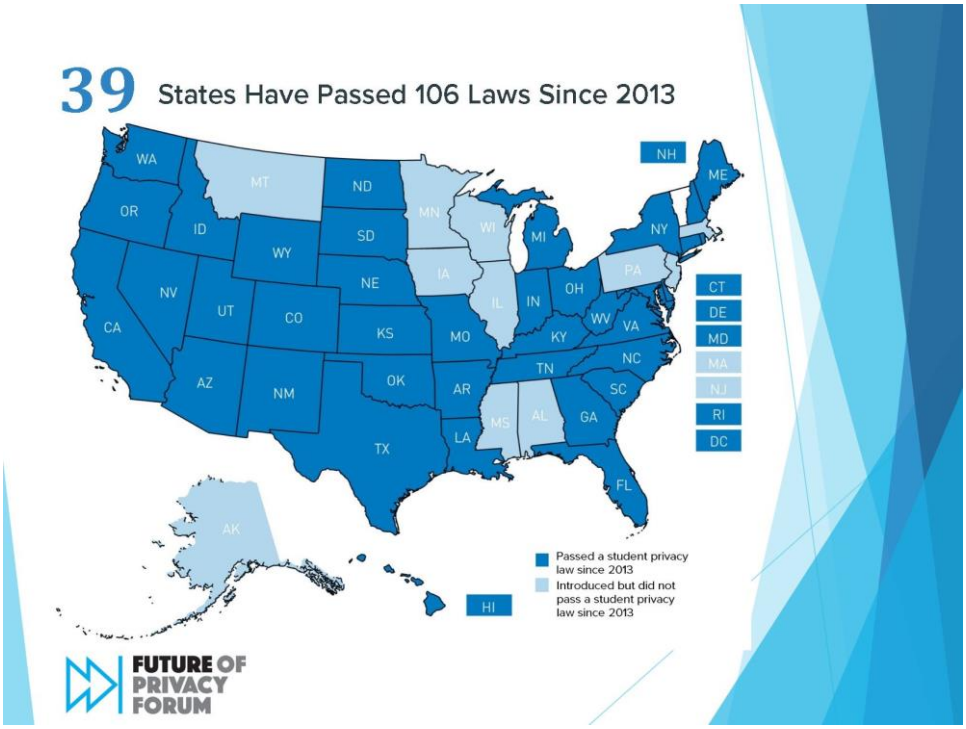
## Why Transparency?

- 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.*








57

## 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



58

## 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:









## KNOW *WHAT* YOU HAVE!!

- What information are you collecting about students?

**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.





# 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.







# 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

How do I protect data?

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





## Do you share information with third parties?

- 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.







## 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







## 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.



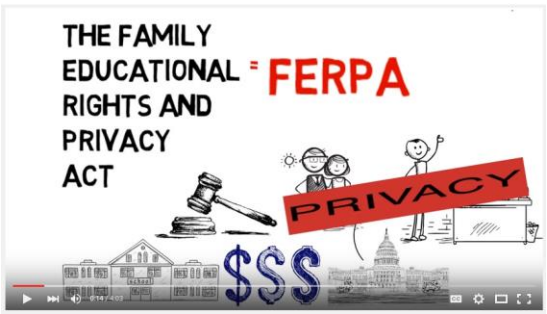






## Recommendations on How to Communicate about Data Practices

- 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







## 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







# Where do I start?

- PTAC Guidance Videos
- Transparency Best Practices











Let's look at some examples…



77

# 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

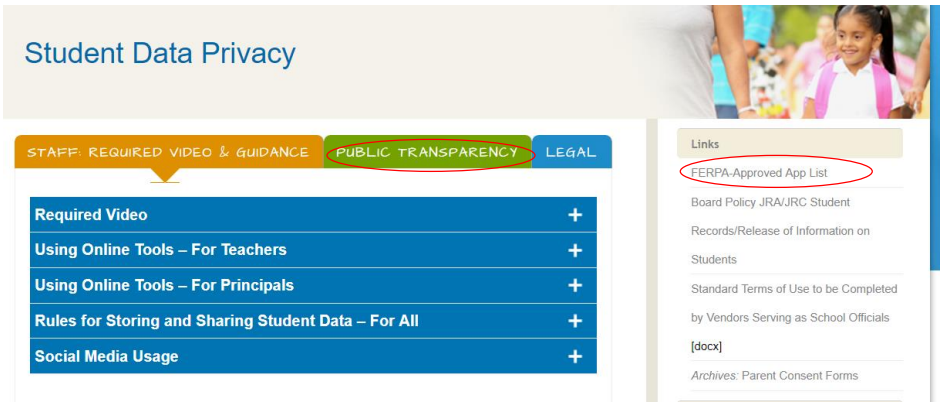
All FCPS stakeholders have the responsibility to use FCPS digital resources in accordance with the law, FCPS regulations, and FCPS best practices guidelines and have rights and responsibilities as follows:

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



78

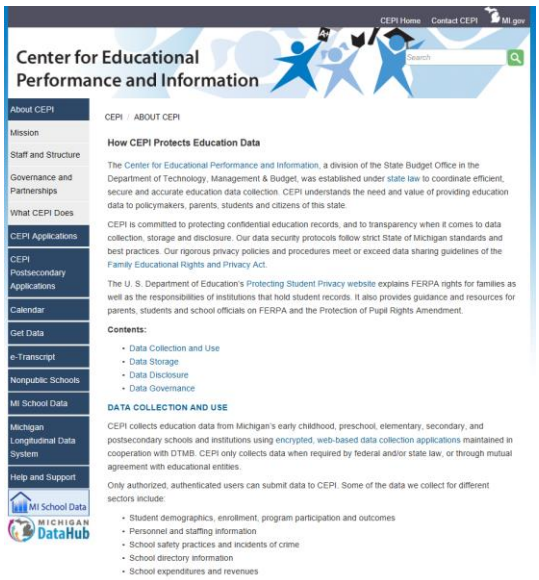
# Denver Public Schools



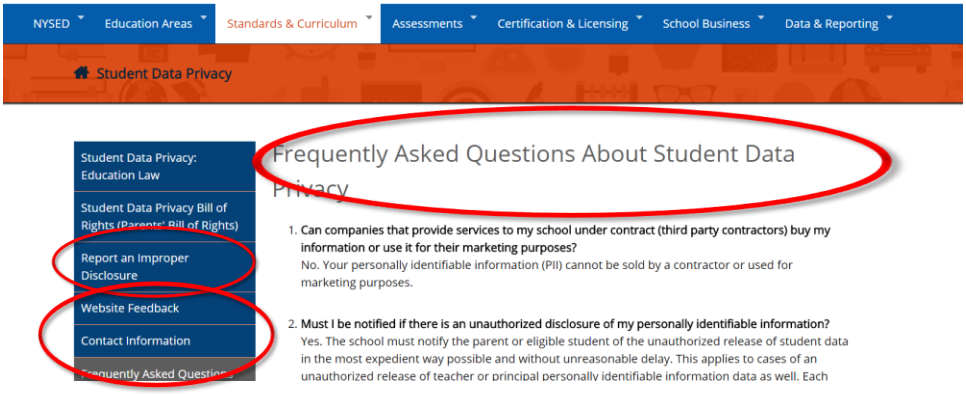





www.michigan.gov/cepi/



# New York State Department of Education

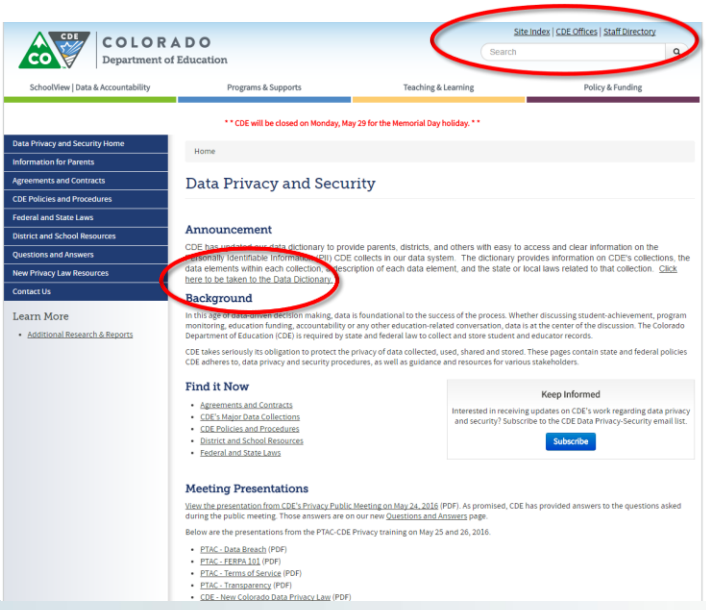






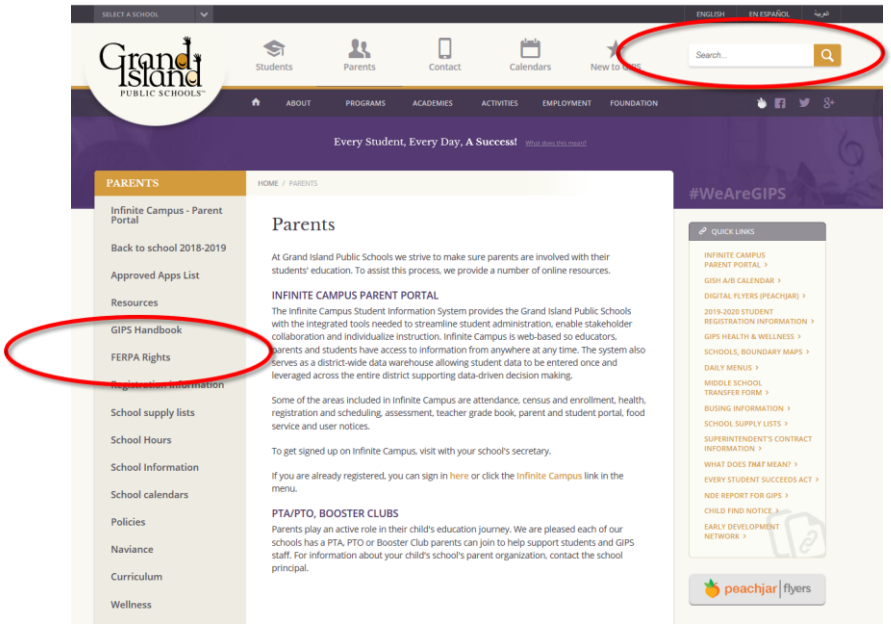



http://www.cde.state.co.us/cdereval/dataprivacyandsecurity





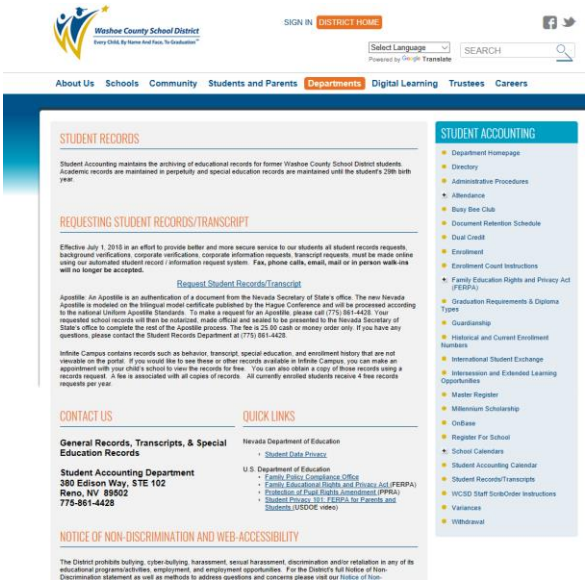




Grand Island PUBLIC SCHOOLS
Students
Parents
Contact
Calendars
ABOUT
PROGRAMS
ACADEMIES
ACTIVITIES
EMPLOYMENT
FOUNDATION
Every Student, Every Day, A Success!
PARENTS
Infinite Campus - Parent Portal
Back to school 2018-2019
Approved Apps List
Resources
GIPS Handbook
FERPA Rights
School supply lists
School Hours
School Information
School calendars
Policies
Naviance
Curriculum
Wellness
Parents
At Grand Island Public Schools we strive to make sure parents are involved with their students' education. To assist this process, we provide a number of online resources.
INFINITE CAMPUS PARENT PORTAL
The Infinite Campus Student Information System provides the Grand Island Public Schools with the integrated tools needed to streamline student administration, enable stakeholder collaboration and individualize instruction. Infinite Campus is web-based so educators, parents and students have access to information from anywhere at any time. The system also serves as a district-wide data warehouse allowing student data to be entered once and leveraged across the entire district supporting data-driven decision making.
Some of the areas included in Infinite Campus are attendance, census and enrollment, health, registration and scheduling, assessment, teacher grade book, parent and student portal, food service and user notices.
To get signed up on Infinite Campus, visit with your school's secretary.
If you are already registered, you can sign in here or click the Infinite Campus link in the menu.
PTA/PTO, BOOSTER CLUBS
Parents play an active role in their child's education journey. We are pleased each of our schools has a PTA, PTO or Booster Club parents can join to help support students and GIPS staff. For information about your child's school's parent organization, contact the school principal.
#WeAreGIPS
QUICK LINKS
INFINITE CAMPUS PARENT PORTAL
GISH A/B CALENDAR
DIGITAL FLYERS (PEACHJAR)
2019-2020 STUDENT REGISTRATION INFORMATION
GIPS HEALTH & WELLNESS
SCHOOLS, BOUNDARY MAPS
DAILY MENUS
MIDDLE SCHOOL TRANSFER FORM
BUSING INFORMATION
SCHOOL SUPPLY LISTS
SUPERINTENDENT'S CONTRACT INFORMATION
WHAT DOES THAT MEAN?
EVERY STUDENT SUCCEEDS ACT
NDE REPORT FOR GIPS
CHILD FIND NOTICE
EARLY DEVELOPMENT NETWORK
peachjar flyers








Washoe County School District
SIGN IN
DISTRICT HOME
Select Language
SEARCH
About Us
Schools
Community
Students and Parents
Departments
Digital Learning
Trustees
Careers
STUDENT RECORDS
Student Accounting maintains the archiving of educational records for former Washoe County School District students. Academic records are maintained in perpetuity and special education records are maintained until the student's 29th birth year.
REQUESTING STUDENT RECORDS/TRANSCRIPT
Effective July 1, 2018 in an effort to provide better and more secure service to our students all student records requests, background verifications, corporate verifications, corporate information requests, transcript requests, must be made online using our automated student record / information request system. Fax, phone calls, email, mail or in person walk-ins will no longer be accepted.
Request Student Records/Transcript
Apostille: An Apostille is an authentication of a document from the Nevada Secretary of State's office. The new Nevada Apostille is modeled on the Intlingual model certificate published by the Hague Conference and will be processed according to the national Uniform Apostille Standards. To make a request for an Apostille, please call (775) 861-4428. Your requested school records will then be notarized, made official and sealed to be presented to the Nevada Secretary of State's office to complete the rest of the Apostille process. The fee is 25.00 cash or money order only. If you have any questions, please contact the Student Records Department at (775) 861-4428.
Infinite Campus contains records such as behavior, transcript, special education, and enrollment history that are not viewable on the portal. If you would like to see these or other records available in Infinite Campus, you can make an appointment with your child's school to view the records for free. You can also obtain a copy of those records using a records request. A fee is associated with all copies of records. All currently enrolled students receive 4 free records requests per year.
CONTACT US
General Records, Transcripts, & Special Education Records
Student Accounting Department
380 Edison Way, STE 102
Reno, NV 89502
775-861-4428
QUICK LINKS
Nevada Department of Education
Student Data Privacy
U.S. Department of Education
Family Policy Compliance Office
Family Educational Rights and Privacy Act (FERPA)
Protection of Pupil Rights Amendment (PPRA)
Student Privacy 101: FERPA for Parents and Students (USDOE video)
NOTICE OF NON-DISCRIMINATION AND WEB-ACCESSIBILITY
The District prohibits bullying, cyber-bullying, harassment, sexual harassment, discrimination and/or retaliation in any of its educational programs/activities, employment, and employment opportunities. For the District's full Notice of Non-Discrimination statement as well as methods to address questions and concerns please visit our Notice of Non-
STUDENT ACCOUNTING
Department Homepage
Directory
Administrative Procedures
Attendance
Busy Bee Club
Document Retention Schedule
Dual Credit
Enrollment
Enrollment Count Instructions
Family Education Rights and Privacy Act (FERPA)
Graduation Requirements & Diploma Types
Guardianship
Historical and Current Enrollment Numbers
International Student Exchange
Intersession and Extended Learning Opportunities
Master Register
Millennium Scholarship
OnBase
Register For School
School Calendars
Student Accounting Calendar
Student Records/Transcripts
WCSD Staff ScribOrder Instructions
Variances
Withdrawal





## Remember this?

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







## Image Redacted

- Visited a sampling of Michigan School District Websites
  - Searched Privacy
  - Searched FERPA
- Some districts did ok
- Some may need improvement





## 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.







## Department 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.





# CONTACT INFORMATION

United States Department of Education,
Privacy Technical Assistance Center

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

privacyTA@ed.gov

https://studentprivacy.ed.gov

(855) 249-3073