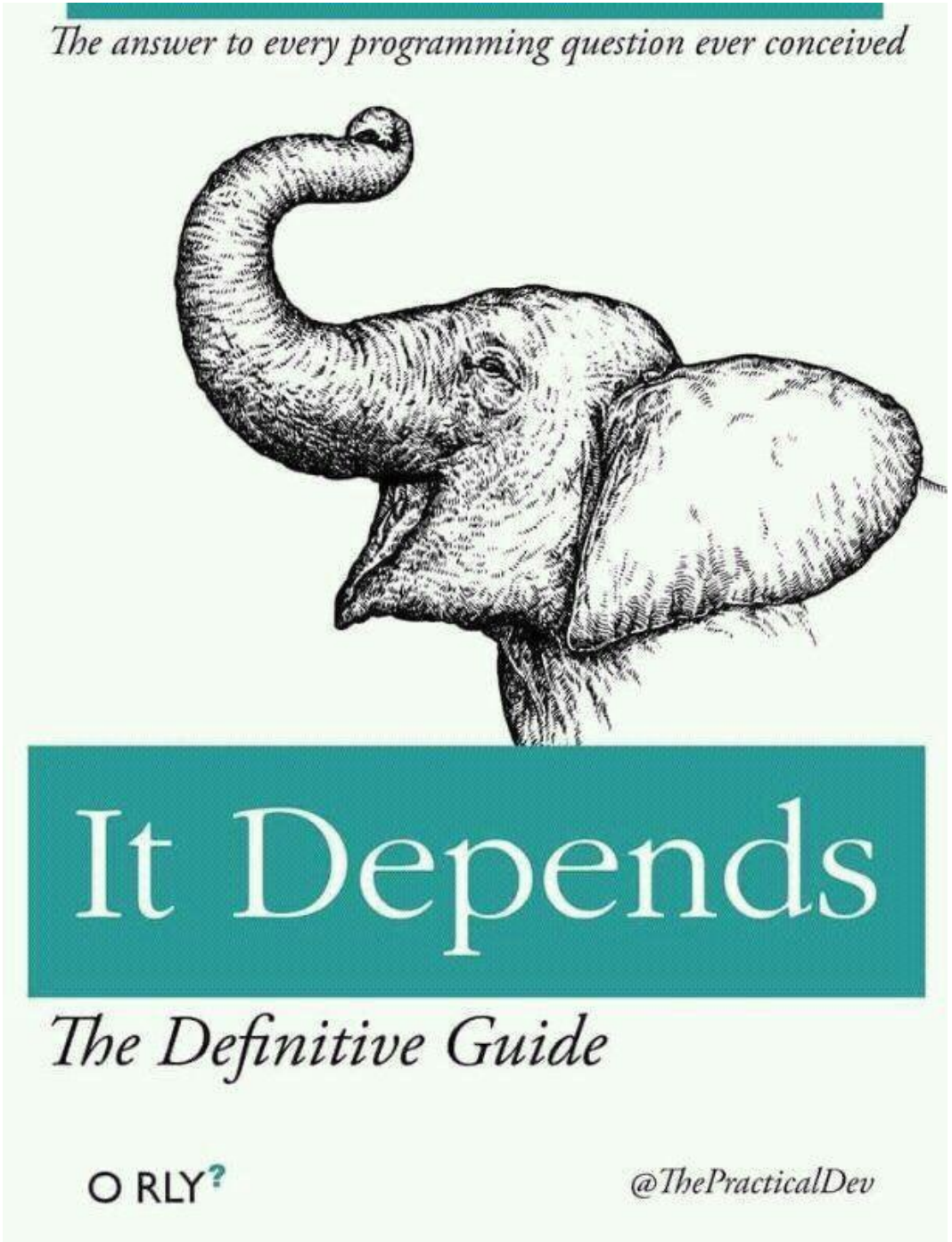
Access 4 Learning Community

STUDENT PRIVACY EDITION

Common Myths, Misinformation and Misunderstandings

Jim Siegl
Senior Technologist
Future of Privacy Forum
jsiegl@fpf.org

*Heard via Lauren Tan



FERPA Myths

Myth: *"In Loco Parentis" means schools/teachers can consent to a student's use of any online services on their parent's behalf, as long as it is for "educational purposes."*

REALITY: FALSE

FERPA provides the parent or eligible student right to consent to the disclosure of education records unless a specific exception applies (e.g. the school official exception).

There is no "In Loco Parentis" exception.

FERPA Myths

Myth: *A vendor can designate themselves as a "school official" by declaring it in their terms, and that means a teacher can use it.*

REALITY: FALSE

It is the school's responsibility to determine the criterial for a school official, who can grant that status(e.g. individual teachers), and if a given service falls under the school official exception.

Related: Can a teacher designate a vendor as a "school official"

FERPA Myths

Myth: *If a vendor is not a "school official", a teacher can still use that vendor's product so long as they give parents (or students) the ability to "opt-out".*

REALITY: FALSE

With the exception of "Directory Information", disclosing data is always OPT-IN unless an exception applies.
A related "myth" is that opting out of directory information overrides the use of any other FERPA exception--also false.

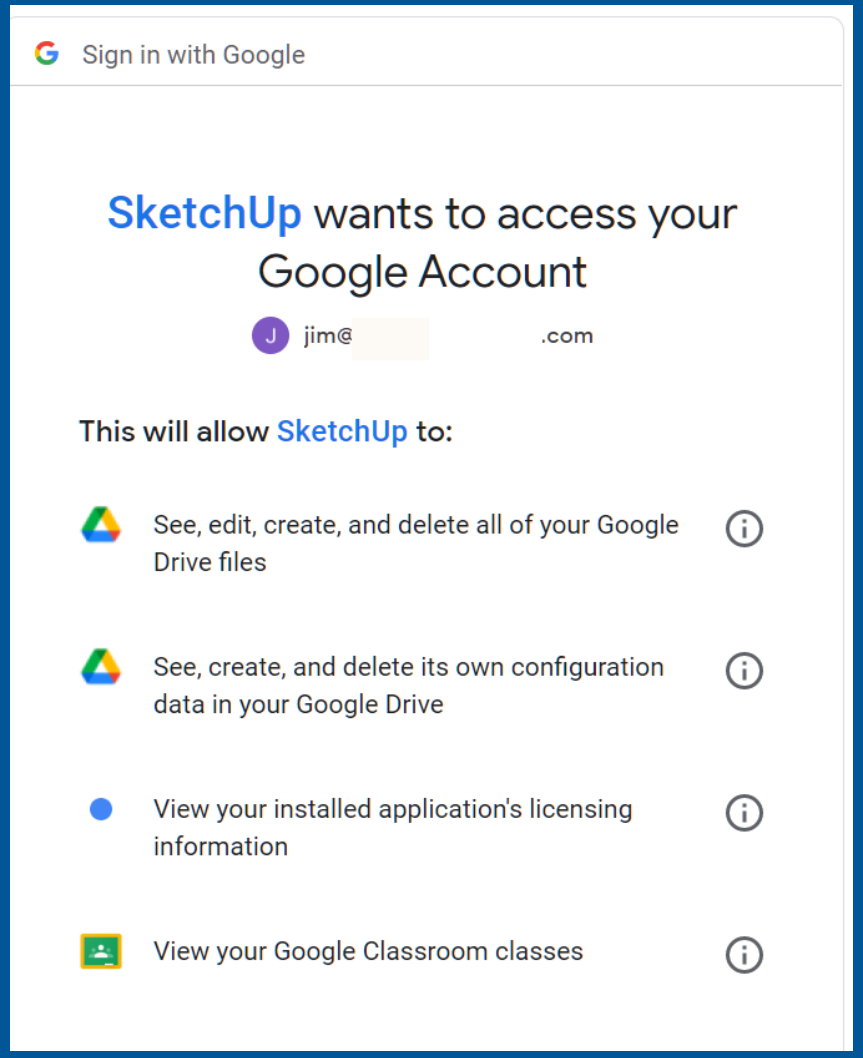
FERPA Myths

***Myth**: Schools only have to have a DPA or get permission if student accounts are being created or the student has to log-in to use the service.*

REALITY: FALSE

FERPA covers the data (the PII) about a student, that is maintained by the school regardless of who creates or uses the account.

Access 4 Learning Community



Technology Myths

***Myth**: "Login with Google" (Microsoft etc. via Oauth2) is not creating an account, you are just "logging in"*

REALITY: FALSE

These service usually do create accounts, they also share data (PII), they will tell the login service that the 3rd party is used (a form of tracking), and most significantly they often grant the 3rd party ability to act on behalf of the user(authorization vs Authentication).

FERPA Myths

Myth: *A vendor has accounts that students create themselves, and are not viewable or managed by the school/teacher, but it is OK since the vendor has signed our Data Protection Agreement as a "school official".*

REALITY: LIKELY SHAKEY GROUND

*In this case, it would be **hard** (not impossible) to argue that the school has established "direct control" over the vendor. It would also be hard to fulfil a parent's request to inspect the student's education record.*

FERPA Myths

Myth: *If an online services needs "only" directory information to sign up, it is OK for schools to sign students up, or have them sign up on their own.*

REALITY: FALSE

Unless the service is literally just a directory, it is likely that any use of the service--even logging in--would create an education record. Also, given this exception's "opt-out" rights, using the directory information exception can create inequities.

FERPA Myths

Myth: *If a vendor says they are "FERPA compliant" or FERPA certified, it is OK to use.*

REALITY: FALSE

It means nothing if a vendor says they are "FERPA compliant." FERPA regulates schools, not vendors, so a vendor proclaiming that they're "FERPA-compliant" on their website or promotional materials is essentially meaningless. "There is no such thing as a 'FERPA seal of approval.'

**However USED has provided guidance on the Responsibilities of Third-Party Service Providers under FERPA.*

Access 4 Learning Community

Myth: *"By privacy law we are not allowed to have digital resources that have advertising."*

REALITY: USUALLY FALSE, BUT PROBLEMATIC

The common language in most state laws refers to behavioral, or target advertising, which would still permit contextual advertising. But telling the difference and monitoring compliance is difficult.

(A broad interpretation of this would likely rule out most news websites and much of the internet as "resources")

COPPA Myths

***Myth**: When a vendor says they are "COPPA compliant" or have a seal from a FTC-approved "safe harbor," that means information is kept private and, therefore, that it is okay to use in my class.*

REALITY: FALSE

COPPA, despite the phrase "privacy protection" in the name, is primarily about parental notice and consent. If the parent provides informed consent then the vendor could use the data in a way that would not be allowed under FERPA without consent.

COPPA Myths

Myth: *Vendors can say in their Terms of Service that schools are* ***responsible*** *for complying with COPPA.*

REALITY: FALSE

The FTC clarified that vendors operators should not state in Terms of Service or anywhere else that the school is responsible for complying with COPPA, as it is the responsibility of the operator to comply with the Rule.

COPPA Myths

Myth: *Vendors subject to COPPA can delegate collecting, managing, and storing of parental permission to schools*

REALITY: REPLY HAZY, ASK AGAIN LATER

The FTC has not weighed in on this yet. Regardless, as a school, COPPA applies to commercial entities (vendors), and you need to follow FERPA, and any state laws which would require you to get consent.

Parental Consent

School Approaches to Consent vary widely

What

- Apply policy to all tools,
  OR
- Apply Policy to all non-contracted tools

Who

- Apply Policy to all students,
  OR
- Apply Policy to all students under 13
  (protects vendor, but not school)

Who Decides

- Decisions / responsibility for permission at the Teacher level
  OR
- Decisions at School or District level (considered Best Practice by DOE/FTC)

How

- Ad-Hoc (separate decision for each tool)
- Get Signatures for nothing (ignore)
- Get Signatures for Everything
- Get Signatures for opt-out
- Get Signatures for “major” tools (e.g. Google Apps, Microsoft Office 365)
- Get Blanket approval (e.g as part of a 1-1 Device initiative or annual Responsible/Acceptable Use Policy)
- Have parent create accounts for <13
- Try to avoid by limiting tools to where district can negotiate contracts with vendors (School official exception)

Parental Consent Myths

Myth: *"Parents will have the opportunity to "opt-out" of their children's use of Supplementary Digital Tools. Accounts are created individually by the teacher or the student, depending on grade level."*

REALITY: COMPLICATED (BUT GENERALLY FALSE)

If PII is collected/shared and not enabled by a FERPA exception (e.g. school official), consent is required. Consent is opt-in, NOT opt-out

Parental Consent Myths

Myth: *FERPA allows a school to have parents provide "blanket consent" for the use of edtech (e.g. as part of the annual AUP).*

REALITY: VERY LIKELY FALSE

FERPA requires that the written consent state the data being shared, the purpose and the party or classes of parties with whom it is being shared.

Parental Consent Myths

Myth: *If a student is 13 or over, teachers don't need to get parental consent.*

REALITY: FALSE

*FERPA, not COPPA applies to schools, and all student ed records, regardless of age. The FTC guidance says that schools **can** provide consent on behalf of parents, ONLY when contracting with a vendor, IF the vendor collects data collects personal information from students for the use and benefit of the school, and for no other commercial purpose.*

IF a product collected PII from students for commercial purposes, FERPA would require written consent.

Which are Valid Forms of FERPA Consent?

A. Paper that the parent signs/dates that lists the app(s)/App vendor, how the school will use it and types of data collected/created.

B. As in “A”, but a Google form the parent types in their name, email and “I accept”,

C. As in “A”, but a form with a unique ID sent to the parent’s email of record,

D. Printed Form that mentions“approved apps”

E. As in “D”,, but an online form with a block to draw a signature

F. Form that lists app(s)/App vendor, how the school will use it and types of data collected/created and allows the parent to opt-out.

G. Form or web page that authenticates the parent using a district credential (e.g. a parent portal) that lists app(s)/App vendor, how the school will use it and types of data collected/created.

H. Paper form that a concurrently enrolled student parent signs/dates that lists the app(s)/App vendor, how the school will use it and types of data collected/created.

Which are Valid Forms of FERPA Consent?

A. Paper that the parent signs/dates that lists the app(s)/App vendor, how the school will use it and types of data collected/created,

B. As in “A”, but a Google form the parent types in their name, email and “I accept”,

C. As in “A”, but a form with a unique ID sent to the parent’s email of record,

D. Printed Form that mentions“approved apps”,

E. As in “D”, but an online form with a block to draw a signature,

F. Form that lists app(s)/App vendor, how the school will use it and types of data collected/created and allows the parent to opt-out,

G. Form or web page that authenticates the parent using a district credential (e.g. a parent portal) that lists app(s)/App vendor, how the school will use it and types of data collected/created,

H. Paper form that a concurrently enrolled student parent signs/dates that lists the app(s)/App vendor, how the school will use it and types of data collected/created,

I. “B” combined with notification (email, phone, text) to the parent confirming their consent (not perfect, but better than the “bad” ones)

Parental Consent

§ 99.30 Under what conditions is prior consent required to disclose information?

(a) The parent or eligible student shall provide a **signed and dated written consent** before an educational agency or institution discloses personally identifiable information from the student's education records, except as provided in § 99.31.

(b) The written consent must:

(1) Specify the records that may be disclosed;

(2) State the purpose of the disclosure; and

(3) Identify the party or class of parties to whom the disclosure may be made.

*See US Department of Education's Identity Authentication Best Practices for ways to verify identity.

HIPAA Myths

Myth: *If it involves student health information, the school and the vendor have to comply with HIPAA.*

REALITY: FALSE

Nearly all health data held by schools is not covered by HIPAA. There is an explicit exception in HIPAA for information covered under FERPA in K12 ed records.

See US ED/HHS Joint Guidance

PPRA Myths

Myth: *If I am surveying students about any of the 8 PPRA categories, I don't have to get consent if the survey is optional, or anonymous.*

REALITY: IT DEPENDS

PPRA is complicated, "not required" participation can be misinterpreted. Anonymity can be "broken" if the survey allows free response options. Even if you are compliant, you may not be aligned with community norms/expectations.

Resource: https://studentprivacycompass.org/faqs-ppra/

The Protection of Pupil Rights Amendment

The Protection of Pupil Right Amendment requires parental notification and/or consent **before** minors can participate in surveys administered by schools that reveal the following **sensitive information**.

1. Political affiliations or beliefs
2. Mental or psychological problems
3. Sex behavior or attitudes
4. Illegal, anti-social, self-incriminating, or demeaning behavior
5. Critical appraisals of family
6. Privileged relationships
7. Religious practices, affiliations, or beliefs
8. Income

PROTECTION OF PUPIL RIGHTS AMENDMENT (PPRA)

Participation Required	Covers the Eight Protected Categories	Opt-in/Opt-out
Yes	Yes	Provide notice, parents must opt in for the student to take the survey
Yes	No	Provide notice and parents have the right to opt out
No	Yes	Provide notice and parents have the right to opt out (but check your specific state law first)
No	No	Provide notice only if the survey was created by a third party. In that case, parents have the right to opt out.

https://studentprivacycompass.org/faqs-ppra

Access 4 Learning Community

The Salt Lake Tribune

After rating students' decency with 'outrageous' drugs and sex quiz, Utah teacher is placed on leave

	27. Have you (your girl) ever had an abortion?	12
	28. Have you (your girl) had more than one abortion?	13
	29. Even though you are straight would you go kinky to see what its like	13
	30. Ever stolen money to buy drugs?	13
	Total:	

Score Chart:	
nder 10	A nerd—just where you should be at your age
11-15	Pure as Ivory soap and maybe a fruitcake
17-20	Passionate but sensible
21-39	Normal and decent
40-75	Indecent
76-85	Headed for serious trouble

FERPA Myths

Myth: *I can share / disclose data as long as it is "deidentified" or agregate data.*

REALITY: IT DEPENDS

Despite deidentification techniques, users can sometimes be reidentified. Examples include: 17% of US 2010 census data, a 2006 Netflix contest, and in a 2021 incident in which anonymized data for 700 million LinkedIn users was scraped from a public dataset and could be used to reveal personal data such as usernames, phone numbers and email addresses

FERPA Myths

Myth: *Staff can use student data to fulfill requiremnts disertation research and data can be shared with universities under FERPA's "Research exception"*

REALITY: FALSE

There is no such thing as FERPA's Research exception.

FERPA: Studies Exception

PII from education records may be disclosed in connection with certain studies conducted “for or on behalf of” schools, school districts, or postsecondary institutions

Studies must be for the purpose of

- Developing, validating, or administering predictive tests;
- Administering student aid programs; or
- **Improving instruction**

There must be a **written agreement** with the individual/organization performing the study that meets certain requirements.

Written Agreements—Studies Exception

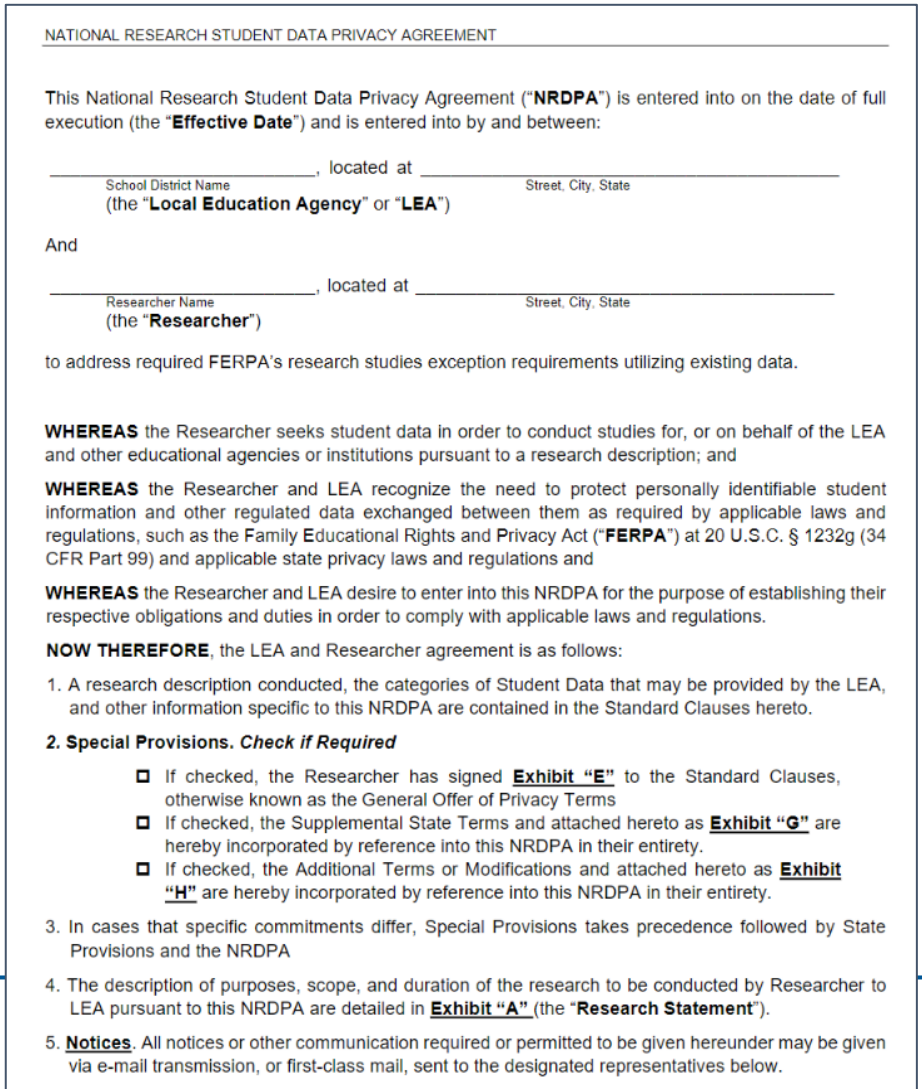
Written agreements must

- Specify the purpose, scope, and duration of the study and the information to be disclosed, and
- Require the organization to
  - **use** PII only to meet the purpose(s) of the study,
  - **(protect) limit** access to PII to those with legitimate interests,
  - conduct the study in a manner that doesn't permit the identification of parents or students by anyone other than representatives of the organization with legitimate interests,
  - **destroy** PII upon completion of the study and specify the time period in which the information must be destroyed

SDPC National Research Data Protection Agreement (NRDPA)

- **What is it?**
  - A Model "written agreement" aligned to FERPA's Studies exception.
  - Intended to be **part of** a district's broader approach to approving research requests.

- **What is it Not?**
  - Does not address non-student data (e.g. employee)
  - Does not address situations where consent is required (e.g. primary data collection from students).
  - Does not address other parts of the research request process.
  - Does not address data use covered under FERPA's audit/evaluation exception.



NATIONAL RESEARCH STUDENT DATA PRIVACY AGREEMENT

This National Research Student Data Privacy Agreement ("**NRDPA**") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between:

_____, located at _____
School District Name — Street, City, State
(the "**Local Education Agency**" or "**LEA**")

And

_____, located at _____
Researcher Name — Street, City, State
(the "**Researcher**")

to address required FERPA's research studies exception requirements utilizing existing data.

WHEREAS the Researcher seeks student data in order to conduct studies for, or on behalf of the LEA and other educational agencies or institutions pursuant to a research description; and

WHEREAS the Researcher and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99) and applicable state privacy laws and regulations and

WHEREAS the Researcher and LEA desire to enter into this NRDPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, the LEA and Researcher agreement is as follows:

1. A research description conducted, the categories of Student Data that may be provided by the LEA, and other information specific to this NRDPA are contained in the Standard Clauses hereto.

2. Special Provisions. ***Check if Required***

- ☐ If checked, the Researcher has signed **Exhibit "E"** to the Standard Clauses, otherwise known as the General Offer of Privacy Terms
- ☐ If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this NRDPA in their entirety.
- ☐ If checked, the Additional Terms or Modifications and attached hereto as **Exhibit "H"** are hereby incorporated by reference into this NRDPA in their entirety.

3. In cases that specific commitments differ, Special Provisions takes precedence followed by State Provisions and the NRDPA

4. The description of purposes, scope, and duration of the research to be conducted by Researcher to LEA pursuant to this NRDPA are detailed in **Exhibit "A"** (the "**Research Statement**").

5. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

Access 4 Learning Community

Myth: It is OK to share FRM (Free and Reduced Meal) information when it provides the student or family a benefit (e.g. reduced Internet access)

REALITY: FALSE

Access within a school only to a limited number of individuals.
State and local laws and policies may apply (e.g. background checks)
Consent required for release – Violations are a criminal penalty.—a fine of up to $1,000 or imprisoned not more than 1 year, or both.

Access 4 Learning Community

Myth: Vendor X is selling student data

REALITY: USUALLY FALSE (But Be Careful)

Even when vendors show targeted ads (prohibited under the school official exception and many state laws even with consent) they are selling "eyeballs" not data. Some products e.g. Life360, do sell data (including location) to data brokers and "trackers" send data to 3rd party sites.

A frequent misunderstanding is the diference between privacy in consumer and EDU version (e.g. Google)

CIPA Myths

Myth: *CIPA, the Children's Online Protection Act, requires schools to track student internet access.*

REALITY: FALSE

Arguably, CIPA (§ 54.520) is not a "privacy law" it requires an interet safety policy that addresses "unauthorized disclosure or personal identification information". It requires a technology that blocks or filters Internet access to content that is obscene, child pornography, [image] harmful to minors .The term "monitor" is not defined, guidance states that it "CIPA does not require the tracking of Internet use by minors or adults"

Access 4 Learning Community

Questions?

Resources for "Research" uses of Student Data

- Forum Guide to Supporting Data Access for Researchers
- Forum Guide to Data Ethics Online Course
- Written Agreement Checklist
- Guidance for Reasonable Methods and Written Agreements
- FAQs: The Protection of Pupil Rights Amendment
- Data Sharing Agreement Checklist for IDEA Part C and Part B 619 Agencies and Program
- Best Practices for Access Controls and Disclosure Avoidance Techniques
- Data De-identification: An Overview of Basic Terms
- **Examples of District Policies for Researcher Access Student Data**
  - Chicago Public Schools Research Study and Data Policy
  - Boston Public Schools
  - Dekalb County School District
  - Fairfax County (VA) (Board Policy)
  - Dallas Independent School District
  - Palm Beach (FL) Board Policy

Contact Information

Jim Siegl
jsiegl@fpf.org

www.fpf.org
www.studentprivacycompass.org
@studentprivacycompass