

Louisiana Believes

Protecting Student Privacy:
Equipping Teachers to Use Educational
Technology Safely

Objectives

In this session participants will

- Explore information teachers need prior to using technology tools
- Review laws and best practices surrounding student data privacy
- Prepare to re-deliver privacy training to teachers

What Do Teachers Need to Know About Using Technology in the Classroom?

Integrating educational applications and digital tools safely, responsibly, and effectively can be a challenge.

1. Know legal and ethical responsibilities
2. Know school system policies and practices
 - Acceptable use policy
 - Online service policy
 - School board privacy policy
3. Utilize best practices

Laws Governing Student Data

Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act (FERPA) is a federal law that affords parents the right to:

- have access to their children's education records
- seek to have the records amended
- have some control over the disclosure of personally identifiable information from the education records.

When a student turns 18 years old, or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student.

Education records are defined as those **records, files, documents, and other materials** that contain information directly related to a student and are maintained by an education agency or institution or by a person acting for such agency of institution. An education record is considered confidential because it contains personally identifiable information about a student.

FERPA Exceptions

Parental consent: must consist of three elements - what data, to whom and what purpose

School officials with legitimate educational interests:

- Schools in which a student seeks or intends to enroll
- In connection with financial aid, such as a college loan
- Directory information (specific guidelines must be followed to utilize this option)

Special Circumstances:

- State and local officials pursuant to a State statute in connection with serving the student under the juvenile justice system
- Complying with a judicial order or subpoena (reasonable effort to notify)
- Health or safety emergency

Research:

- Authorized representatives of Federal, State, and local educational authorities conducting an *audit, evaluation, or enforcement of education programs*
- Organizations conducting *studies* on behalf of schools

Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act (COPPA) is a federal law governed by the Federal Trade Commission (FTC). COPPA assures that children under 13 years of age do not share personal information on the Internet without the express approval of their parents.

Providers must obtain consent from parents to collect information, unless they are collecting on behalf of the LEA or school and will only use the information to provide services to the LEA or school. If this is the case, then the provider can rely on consents obtained from the LEA or school. LEAs can consent on behalf of a parent for educational purposes.

Personal Information as Defined by COPPA

- A first and last name
- A home or other physical address including street name and name of a city or town
- Online contact information as defined in this section
- A screen or user name where it functions in the same manner as online contact information, as defined in this section
- A telephone number
- A social security number
- A persistent identifier that can be used to recognize a user over time and across different websites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier
- A photograph, video, or audio file where such file contains a child's image or voice
- Geolocation information sufficient to identify street name and name of a city or town
- Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described above

LA RS 17:3913 (Act 677 of 2014)

Mandates that the LDOE publicize on Louisiana Believes any sharing of students' personally identifiable information and publish new data-sharing agreements within ten days of their execution. LEAs must make the same information about their data sharing available upon request.

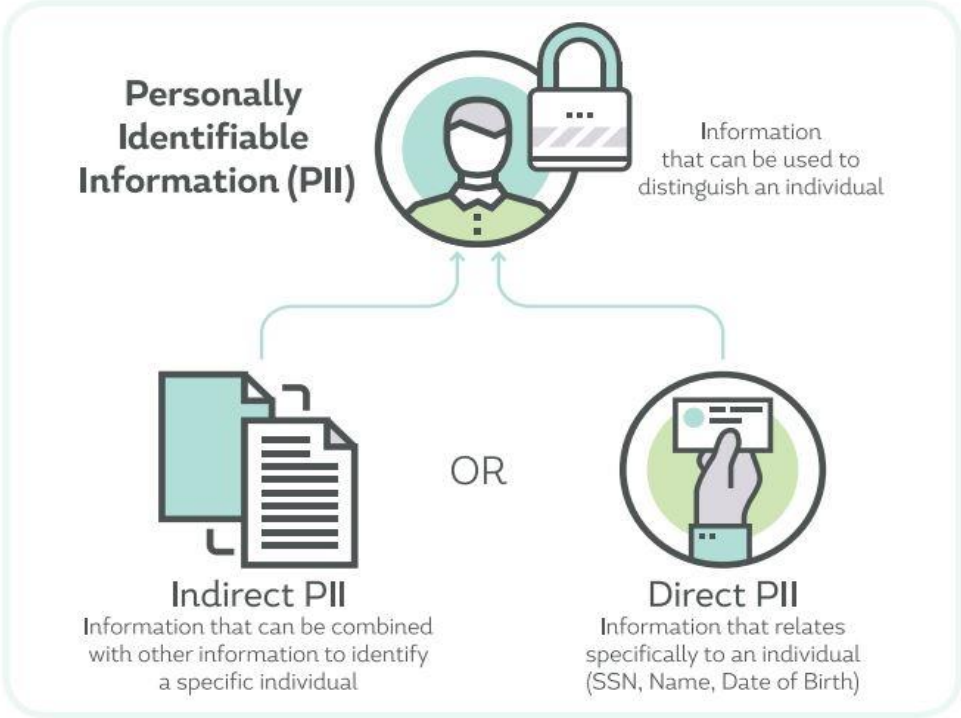
LA RS 17:3914 (Act 837 of 2014)

School Systems are restricted from sharing students' personally identifiable information (e.g. **full name, date of birth, social security number**) with any public or private entity unless it meets one of the law's limited exceptions:

- **LEA Superintendent/Charter Leader Authorization** – A person authorized by a LEA superintendent to perform his duties pursuant to LEA policy.
- **Parental or Legal Age of Majority Consent** – A parent gives written consent to share PII for a specific purpose.
- **Audit** - A person authorized by the state to perform audits, including enrollment counts.
- **Transfer of Student Records** —A student transfers to another school system and records are transferred as described in LA RS 17:112.

If an employee knowingly **shares** PII for purposes other than the exceptions provided in law, he/she is subject to criminal and financial penalties.

Personally Identifiable Information



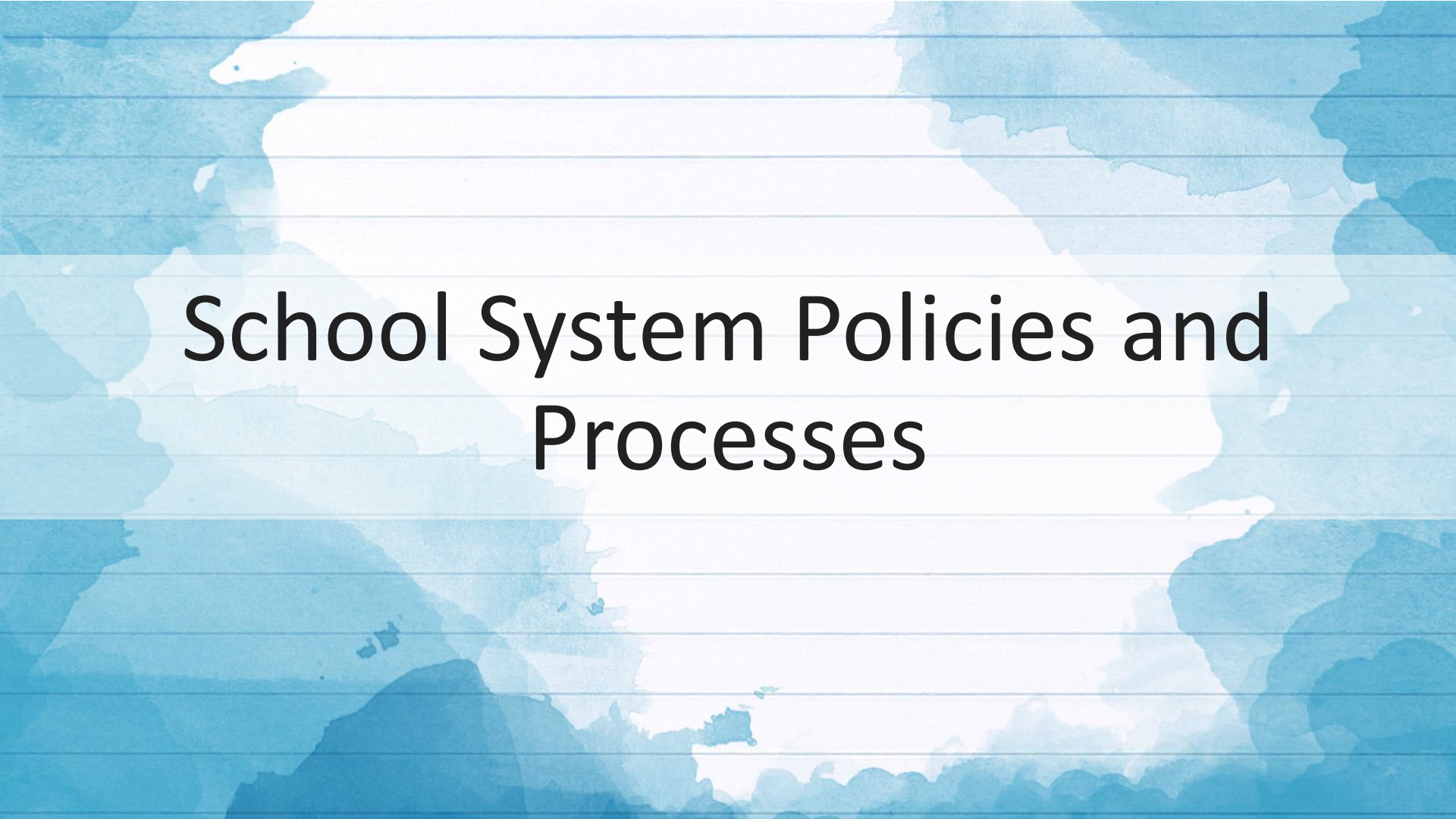
Sensitive PII

Although all PII is protected, some PII is considered sensitive information because if it is lost, exposed to unauthorized parties, or misused, there could be an adverse impact for the individual.

The combination of two or more pieces of non-sensitive PII may result in sensitive information, as when a person's full name is associated with their date of birth and mother's maiden name—information often used to verify a person's identity for credit purposes. Both the potential for harm and the context in which the information is used are important determinants of what constitutes “sensitive” PII.

Turn and Talk

How does your school system communicate student data privacy laws to your teachers?



School System Policies and Processes

School Board Policy

Make It Your Own

Insert information about school board policy.

Online Services

Make It Your Own

Insert school system's policy regarding use of online services and free applications.

Acceptable Use Policy

Make It Your Own

Reinforce acceptable use policy for teachers and for students.

Garner signatures for acceptable use policy.

Turn and Talk

1. Describe your school board policy, online services policy, or acceptable use policy.
2. What other student data policies do you have?

Best Practices

Best Practices to Protect Every Day Use of Student Data

- **Protect visibility** of reports and computer monitors when displaying and working with confidential information.
- **Lock or shut down workstations** when left unattended for any amount of time.
- **Store data in a secure location.** Physical data (including hard copies of reports, storage media, notes, backups) should be protected from unauthorized persons, or locked away when not in use.
- **Transmit sensitive data securely.** This may be done using Secure File Transfer Protocol (sFTP) or encrypted email. Faxing confidential data is not recommended since it poses many security risks.
- **Stamp or otherwise mark confidential** reports or media containing confidential information prior to their release. The envelope containing the information should also indicate that the contents are confidential.
- **Protect user names and passwords:** If using an online educational program which establishes individual log-in information for students such as usernames and passwords, keep them in a private, secure location and teach students to keep their personal log-in information private.

Click-Wrap or Click-Through Agreements

Click-wrap or click-through agreements are when an end-user enters into an agreement by clicking “OK” or “AGREE,” and are very unlikely to have actually read through the entirety of the agreement presented. When using an online tool that relies on a click-wrap agreement:

- check amendment provisions,
- print and save the terms of service,
- develop a policy for use of these types of tools, and
- develop a list of approved tools.

Make It Your Own

Adjust as necessary to align with your school system online services policy.

Using Online Services without Sharing Student Information

Student PII cannot be shared without parental consent or a data sharing agreement. Therefore, when using approved online services one of the two must be in place or de-identified data must be used.

De-identified data possibilities

- Use an alias
- Use initials

Note: Ensure that the student will not be entering PII when using the application.

Make It Your Own

Adjust as necessary to align with your school system online services policy.

Turn and Talk

What are some other best practices that should be communicated?

Resources

Resources

- Acceptable Use Policies
 - [Ascension Parish School Board](#)
 - [NCES](#)
- School Board Policies
 - [St. Tammany \(pg. 6-10\)](#)
- [Louisiana Data Governance and Student Privacy Guidebook](#)
- [Parental Consent](#)
- Contracts or Memorandums of Understanding
 - [Sample Contract Language](#)
 - [MOU Routing Template](#)
 - [Data Release Checklist](#)
 - [Software tracker](#) – Ascension Parish School Board
 - [Contract Information Form](#) – Ouachita Parish School Board
 - [Website Application for Approval](#) – St. Tammany Parish School Board

Contact Information

Kim Nesmith, M.Ed.

Data Governance and Privacy Director

Kim.Nesmith@la.gov