LOUISIANA DEPARTMENT OF EDUCATION

Office of Teaching and Learning

Student Privacy Laws for Staff

In the digital age, protecting student information has become paramount. As educators, it's crucial to be familiar with the various privacy laws and regulations that apply to K-12 institutions. This document outlines key aspects of FERPA, COPPA, CIPA, and other notable privacy laws.

Vocabulary to Know:

- **PII** (Personally Identifiable Information): This includes but is not limited to first and last name, address, phone number, social security number, and biometric data (e.g., fingerprint). Indirect PII includes information that, when combined, would make the student's identity traceable.
- **AUP** (Acceptable Use Policy): A document that stipulates what a user may and may not do when using a school device or Internet services provided by a school.
- **LEA** (Local Education Agency): Public board of education or other public authority legally constituted within a State for administrative control or to perform a service function for schools or school systems.

✓	✗
✔ Make sure students have a **signed AUP** on file before allowing them to use school devices or the Internet. ✔ Check your school system's website for a list of contracted online services and tools to ensure students' privacy will be protected. ✔ Teach students digital citizenship best practices, such as creating strong passwords and password security. ✔ **Monitor** students' technology and Internet use. ✔ Always **lock your devices** when you step away and tell students to do the same to prevent unauthorized access to private information. ✔ **Inform parents** about what tech tools and sites their students are using and what information these sites collect and get their written consent. ✔ **Educate yourself** about updates to student privacy laws and policies.	✖ **Do not** allow students to create logins for online programs without checking if the site has a contract with your school system to protect PII. ✖ **Do not** create logins for students without checking if the site has a contract with your school system to protect PII. ✖ **Do not** use students' names, initials, or other PII to create logins for acceptable sites. ✖ **Do not** create lists of student login information and leave them in easily accessible places.

1. FERPA (Family Educational Rights and Privacy Act)

Overview:
FERPA protects the privacy of student education records.

Key Points for Educators:

- Schools must have written permission from parents or eligible students (those over 18) to release any information from a student's education record.
- Parents or eligible students have the right to inspect and review the student's education records maintained by the school.
- Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must inform parents and eligible students about directory information and allow them a reasonable amount of time to request that the school not disclose directory information about them.

2. COPPA (Children's Online Privacy Protection Act)

Overview:
COPPA applies to websites and online services targeted to children under 13. It ensures that these sites and services protect children's privacy and give parents control over what information websites can collect from their children.

Key Points for Educators:

- If using online tools in the classroom, ensure that they comply with COPPA or that parental consent has been obtained.
- Be wary of apps or websites that request excessive personal information from students.
- Educate students about the importance of not sharing personal information online without parental consent.

3. CIPA (Children's Internet Protection Act)

Overview:
CIPA requires schools and libraries to filter and monitor the activities of minors on computers, especially concerning materials that are obscene or harmful to minors.

Key Points for Educators:

- Ensure that school-provided internet connections have appropriate filtering mechanisms.
- Educate students about safe online behavior and the risks of harmful online content.
- Regularly review and update filtering tools to address the evolving nature of online content.

4. Other Relevant Privacy Laws:

- PPRA (Protection of Pupil Rights Amendment): Protects student privacy in the context of specific physical exams and surveys.
    - Educators should obtain parental consent before any non-emergency, invasive physical examination or any survey funded by the U.S. Department of Education.

- LA R.S. 17:3914: Requires the local education agency (LEA) to assign unique identifiers to all students and to track parental consent to share Personally Identifiable Information (PII) with the Louisiana Office of Student Financial Assistance (LOFSA).
    - All students are assigned a Student Identification Number (SIDNO).
- Louisiana Act 677: Requires LEAs to make information about any sharing of students' PII available at the main office of the governing authority.
- LA RS 17:3914 Louisiana's Student Privacy Law[1]: Provides limitations and prohibitions on collecting and sharing student information.
    - LEAs cannot require the collection of non-academic data such as political affiliation or religious practices.
    - LEAs cannot share PII with external entities unless a parent has given written consent or sharing meets one of the law's limited exceptions (see footnote 1).

Best Practices:

- **Stay Updated**: The digital landscape is rapidly changing. Ensure you are up to date on new laws and modifications to existing ones.
- **Educate Students:** Incorporate digital citizenship lessons into the curriculum to teach students about online safety and privacy.
- **Parental Engagement:** Regularly communicate with parents about the tools and platforms being used in the classroom, their privacy implications, and any necessary consents.
- **Protect Visibility:** Lock or shut down workstations when left unattended for any amount of time and make sure that computer monitors displaying confidential information are protected from public view.
- **Secure Data Storage**: Keep physical copies of data locked away and protected, and keep passwords (both for educators and students) in private, secure locations.
- **Check PII Agreements:** Each school system should have a published list of vendors with whom they have contracts or PII agreements and are deemed safe for students to log in to (e.g., Calcasieu Parish, Livingston Parish, State of Louisiana).

Protecting the privacy of students is not just a legal requirement but a fundamental responsibility of educators in the 21st century. By understanding and adhering to these laws, educators ensure a safe and conducive environment for students to learn and thrive.

Note: This document provides a general overview and may not cover every detail of the laws mentioned. Always refer to official documents or legal counsel for comprehensive guidance.

[1] LDOE Student Privacy Planning Guide