Summary

DATA TRANSFER | Only transmit personally identifiable information (PII) in secure ways e.g. sharing files using a Secure File Transfer Protocol (SFTP) or encrypting attachments.

VIDEO CONFERENCE/VIRTUAL LEARNING SOFTWARE APPS | FERPA does not require an educational agency or institution to enter into an agreement under the school official exception, although it is a best practice to clarify the issues of direct control (regarding the use and maintenance of education records or PII) and legitimate educational interest.

- Consider agency or institution's process to review requests for software
- FERPA doesn't address which apps can be used. Work with your information security officers and attorneys to review information security requirements and the platform's Terms of Service.
    - Model Terms of Service
- Look for products that apply best practices like encryption, strong identity authentication, and a statement and terms of service that explain how the vendor's use of PII from student education records complies with FERPA.
- Resources:
    - Protecting Student Privacy While Using Online Educational Services
    - Data Security Checklist

CLASSROOM OBSERVATION | Determination of who can observe a virtual classroom, similar to an in-person classroom, is a local school decision as teachers generally do not disclose personally identifiable information from a student's education record during classroom instruction. It is best practice to discourage non-students from observing virtual classrooms in case PII from a student's education record is disclosed.

RECORDING LESSONS | Teachers can make a recording of the lesson available to students enrolled in the class as long as the video recording does not disclose PII from student education records[1] or appropriate written consent is obtained.

- Check current vendor agreements to determine whether video recordings of virtual classroom lessons are or will be maintained as education records beyond the period of instruction, and if so – how, and by whom.

ACCESS TO RECORDS | Schools should review administrative functions and processes for working with parents to provide access to their child's education record within 45 days.

- This is also true when a provider maintains a student's education records.

[1] "Education records" are, with certain exceptions, directly related to a student and maintained by an educational agency or institution or by a party acting on behalf of the educational agency or institution

- Electronic consent is allowed as long as it (a) identifies and authenticates a particular person as the source of the electronic consent; and (b) Indicates such person's approval of the information contained in the electronic consent.

PARENT-STUDENT CONFERENCES | A teacher's spouse is allowed to be in the same room for a parent-student conference as long as no PII from the student's education record is disclosed in the hearing of the spouse or prior consent is obtained in writing from the parent or eligible student for the potential disclosure of PII from the student's education records to his or her spouse.

Sources: FERPA and Virtual Learning During Covid-19; Protecting Student Privacy When Using Online Educational Services

Best Practices for Protecting Student Privacy When Using Online Educational Services

- **Maintain awareness of other relevant federal, state, tribal, or local laws.**
  - Children's Online Privacy and Protection Act (COPPA)
- **Be aware of which online educational services are currently being used in your district.**
  - Conduct an inventory.
  - A master list of online educational services will help school officials to collaboratively evaluate which services are most effective and help foster informed communication with parents
- **Have policies and procedures to evaluate and approve proposed online educational services (even if free).**
  - School and district-wide policies and processes that are clearly communicated to teachers and administrators.
  - Applies to formal contracts and to consumer-oriented "Click-Wrap" software that is acquired simply by clicking "accept" to the provider's Terms of Service.
- **When possible, use a written contract or legal agreement.**
- **Extra steps are necessary when accepting Click-Wrap licenses for consumer apps.**
- **Be transparent with parents and students about how the school or district collects, shares, protects, and uses student data.**
- **Consider that parental consent may be appropriate even in instances where FERPA does not require parental consent.**

Source: Protecting Student Privacy When Using Online Educational Services

Other Recommendations

- **Streamline systems as much as possible.**
  - E.g.: Connecticut's Commissioner Cardona issued a guidance stating that districts may bypass the process of crafting individual contracts for new

technology solutions that fall under the data privacy statute. Instead, they can use educational technology from companies that have provided digital assurances that they comply with Connecticut's law by signing the Connecticut Student Data Privacy Pledge and providing documentation to support their compliance (e.g., sample contract, data privacy agreement, or addendum documents).
    - Educators can then search their portal for educational software developed by companies that have pledged compliance.
- **Be explicit about the importance of privacy and provide clear guidance.**
    - If you provide a planning template, include requirements for or considerations of privacy and security. Additionally, provide examples of what ensuring internet safety, privacy, and security looks like or simply state your requirements.
    - The same logic applies to other tasks such as teleconferencing, transport of data, etc. Clearly state the importance of and expectations for data security and privacy, and then provide recommendations for how to ensure this.
    - Resources: Essential Cybersecurity Practices for K12; Protecting Students' Online Privacy
- **When providing a list of resources, note whether they have been vetted for FERPA or state compliance**
    - Sample language from New Hampshire: "**The Department of Education has not vetted the below resources for compliance with New Hampshire minimum standards for privacy and security under RSA 189:66 or any relevant state or federal statutes, including but not limited to the ADA, FERPA, HIPAA,. Schools are advised to review all apps and websites for compliance.*"
- **Provide clear guidance around the distribution of student login information.**
    - Sample language from Alabama: "*Take precautions while distributing students' usernames and passwords to parents in order to keep them secure. Note possible options below: ✓ To authenticate, use information both you and the parents know. ✓ One option is to text the parents the password, and then force the password to be changed on the first login. If the parents cannot accept texts, call them and give the password over the phone. ✓ Avoid emailing usernames and passwords in the same email. You could email the username with a message that says you are sending out the password via text. ✓ If there is no phone on file, sending parents a letter in the mail is much safer even though it is a slower process.*"
- **Review and revise policies, procedures, and notifications under FERPA and PPRA in light of COVID-19. To improve transparency of information on student privacy, post this information on your website.**

Glossary

- Children's Online Privacy and Protection Act (COPPA)
    - Absent an exception, commercial Web sites and online services directed to children and those Web sites and services with actual knowledge that they have collected personal information from children must obtain verifiable parental consent prior to collecting personal information from children. In limited circumstances, schools may exercise consent on behalf of parents
- Direct Control
    - While FERPA regulations do not require a written agreement for use in disclosures under the school official exception, in practice, schools and districts wishing to outsource services will usually be able to establish direct control through a contract signed by both the school or district and the provider. In some cases, the "Terms of Service" (TOS) agreed to by the school or district, prior to using the online educational services, may contain all of the necessary legal provisions governing access, use, and protection of the data, and thus may be sufficient to legally bind the provider to terms that are consistent with these direct control requirements.
- Directory information
    - Information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed e.g. name, address. To disclose student information under this exception, individual school districts must establish the specific elements or categories of directory information that they intend to disclose and publish those elements or categories in a public notice.
    - Parents (and eligible students) generally have the right to "opt out" of disclosures under this exception
- Education Records
    1. Directly related to a student; and
    2. Maintained by an educational agency or institution or by a party acting for the agency or institution"
- Personally Identifiable Information (PII)
    - Includes direct identifiers (such as a student's or other family member's name) and indirect identifiers (such as a student's date of birth, place of birth, or mother's maiden name)
- Protection of Pupil Rights Amendment (PPRA)
    - Requires that a school district must, with exceptions, directly notify parents of students who are scheduled to participate in activities involving the collection, disclosure, or use of personal information collected from students for marketing purposes, or to sell or otherwise provide that information to others for marketing purposes, and to give parents the opportunity to opt-out of these activities.

Subject to the same exceptions, PPRA also requires districts to develop and adopt policies, in consultation with parents, about these activities.
    - PPRA has an important exception, however, as neither parental notice and the opportunity to opt-out nor the development and adoption of policies are required for school districts to use students' personal information that they collect from students for the exclusive purpose of developing, evaluating, or providing educational products or services for students or schools.
    - PPRA is invoked when personal information is collected from the student. The use of online educational services may give rise to situations where the school or district provides FERPA-protected data to open accounts for students, and subsequent information gathered through the student's interaction with the online educational service may implicate PPRA
- School Official Exception: Under the school official exception, schools and districts may disclose PII from students' education records to a provider as long as the provider:
    1. Performs an institutional service or function for which the school or district would otherwise use its own employees;
    2. Has been determined to meet the criteria set forth in in the school's or district's annual notification of FERPA rights for being a school official with a legitimate educational interest in the education records;
    3. Is under the direct control of the school or district with regard to the use and maintenance of education records;
    4. 4. Uses education records only for authorized purposes and may not re-disclose PII from education records to other parties (unless the provider has specific authorization from the school or district to do so and it is otherwise permitted by FERPA).