



District Considerations for Protecting Personally Identifiable Information & Protecting Children Online While Working Remotely

School district staff routinely handles sensitive information protected by [HIPAA](#) and [FERPA](#). Additionally, educators working with students online must adhere to both [CIPA](#) and [COPPA](#). Working remotely may involve using new technologies and finding creative ways to utilize existing tools. Administrators and staff should carefully consider any newly adopted means of storing or transferring information, within the context of the responsibility to protect sensitive data.

Protecting personally identifiable information (PII) is a major component for complying with HIPAA, FERPA, and COPPA. While the term itself and legal definitions can vary depending on specific context, for discussions involving remote work and technology, both decision makers and teaching staff should familiarize themselves with the following definition.

Personally Identifiable Information (PII)

Personally identifiable information in the information technology industry is commonly defined as any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (Source: National Institute of Standards and Technology)

Best Practices for Protecting PII and Students While Working Remotely

- Ensure all staff who handle PII are familiar with what constitutes PII and the district procedures for storing and transferring data securely
 - See table below for common secure versus non-secure communication methods below
- Ensure all staff who handle sensitive data are up –to date on, or have recently reviewed, compliance training courses applicable to their areas of responsibility
 - See overviews for applicability and training references by law in the [Quick Reference for Privacy Laws](#) on the next page
 - Teaching staff need to be familiar with both [FERPA](#) and [CIPA](#) guidelines
- Consult with your IT department and vendors to review security concerns when considering adoption of any new online tool or when using an existing tool in a new way where PII is concerned
- Establish support channels for staff for both policy “What should I?” and technology “How do I?” questions
- Plan to implement measures to monitor staff compliance and address issues as they are identified
 - Identifying and addressing the root causes of compliance violations can be challenging in the typical school environment. Anticipate that extended remote work will bring new challenges and considerations

Common Secure Vs. Common Non-Secure Communication Methods

Frequently Approved for PII	Typically Not Approved for PII
District-issued cloud storage accounts	Personal cloud accounts, sharing public links
Internal emails	Personal email accounts
Internal to external encrypted email	Internal to external email without encryption
Telephone calls (non-recorded)	Recorded telephone calls or video conference meetings in Zoom, WebEx, etc.
Secure fax (badge or PIN required to release fax)	Personal/home office fax
District cloud suite – Teams/Group Conversations	Text messages, Zoom, personal Skype, or similar chats

School District Quick Reference for Privacy Laws

HIPAA

Health Insurance Portability and Accountability Act of 1996 (HIPAA) – Federal law created primarily to modernize the flow of healthcare information, stipulate how Personally Identifiable Information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations on healthcare insurance coverage. (Source: hipaaguide.net)

- It may be advisable for staff working remotely with staff or student health records to review the HIPAA course content hosted on Public School Works. (See course: M-229 within “Available Courses”)
- If your district uses another platform for staff training, it is likely it provides a very similar course

Official HIPAA resources for professionals can be found on the HHS website [here](#).

FERPA

Family Educational Rights and Privacy Act of 1974 (FERPA) – Federal law that governs the access to educational information [including personally identifiable student information] and records by public entities such as potential employers, publicly funded educational institutions, and foreign governments. (Source: 20 U.S.C. § 1232g)

- It may be advisable for teaching staff working remotely to review the FERPA course content hosted on Public School Works. (See course: M-152 within “Available Courses”)
- If your district uses another platform for staff training, it is likely it provides a very similar course

Official FERPA resources for educators can be found on the USDOE website [here](#).

CIPA

The Children’s Internet Protection Act of 2000 (CIPA) – Federal law enacted by Congress in 2000 to address concerns about children’s access to obscene or harmful content over the Internet. (Source: FCC)

- It may be advisable for teaching staff working remotely to review the CIPA course content hosted on Public School Works. (See course: M-486 within “Available Courses”)
- If your district uses another platform for staff training, it is likely it provides a very similar course

Official CIPA resources for educators can be found on the FCC website [here](#).

COPPA

Children’s Online Privacy Protection Act of 1998 (COPPA) – Federal law which details what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent or guardian, and what responsibilities an operator has to protect children’s privacy and safety online including restrictions on the marketing of those under 13. (Source: FTC)

Resources that may be helpful to school administrators while considering the use of online tools for students during school closures can be found below.

- [The Educator’s Guide to Student Data Privacy](#)
- [Vetting Online Tools: Start with Privacy](#)
- [Security Questions to Ask of an Online Service Provider](#)

Official COPPA resources for professionals can be found on the FTC website [here](#).