

Data Privacy & Safeguarding Data

Tips for Safeguarding Data



- Never leave documents with personally identifiable information unattended on a desk, network printer, fax machine, or in any place accessible to the general public.
- Never share or give out account information.
- Always lock your computer screen when leaving the workstation.
- Never discuss Personally Identifiable Information over the phone.
- Do not store PII on laptops, personal electronic devices, flash drives, or external hard drives unless the device(s) are encrypted.
- Do not use personal devices to access Personally Identifiable Information.
- Documents containing Personally Identifiable Information should not be sent via interoffice mail.
- Documents containing Personally Identifiable Information should never be thrown in the trash; they should be shredded as soon as they are no longer needed.
- Do not post documents with Personally Identifiable Information on a shared drive or location accessible to others.



- Always check with your district for other policies and procedures when dealing with Personally Identifiable Information.

Federal & State Privacy Laws



Family Educational Rights & Protection Act

Federal law on the privacy of students' educational records, FERPA safeguards student privacy by limiting who may access student records, specifying for what purpose they may access those records, and detailing what rules they have to follow when accessing the data.

Children's Online Privacy & Protection Act

COPPA regulates how commercial entities may collect and use information collected online from children under the age of 13, including the rules about parental consent.

Health Insurance Portability & Accountability Act

HIPAA establishes privacy and security rules regarding access to protected health information in certain kinds of health records, including health plans, health care clearinghouses, and health care providers. Health information about a student appears in an education record, FERPA governs the protection of the data, not HIPAA.

Protection of Pupil Rights Amendment

PPRA defines the rules states and districts must follow when administering tools like surveys, analyses, and evaluations funded by the US Department of Education to students. It requires parental consent to administer many tools and ensures school districts have policies in place regarding how the data collected through these tools can be used.

Children's Internet Protection Act

CIPA requires K-12 schools and libraries receiving federal discounts for internet access to implement internet safety policies that prevent students from accessing inappropriate and/or harmful material and protect against the unauthorized disclosure, use and dissemination of minor's personal information.

Student Online Personal Information Privacy Act

Governs how online service providers can collect, access, and use student data and prohibits online service providers from using student data for commercial or secondary purposes, while still allowing for personalized learning and service innovation and improvement. This law will allow educators to use online services while still safeguarding student privacy.

QUESTIONS?



For more information please visit www.arkansased.gov/divisions/research-and-technology/data-privacy or contact Holly Glover at 501-683-4230