SETIP
Educational Technology Integration Pointers

Student Data Privacy

CIPA, FERPA, NDPA oh my!

It is extremely important to be sure our student's data is being kept private, especially while they are working online for school purposes. Laws have been passed and will continue to pass that legally require schools to protect their students as technology continues to change! Teachers need to be aware of this concern, and they need to be sure they are not using a site that leaks private information.

This seems like yet another thing to put on a teacher's plate, but do not worry! We are going to provide you with information to help pick the safest websites for your students!

Going forward, S3 Technologies will only be recommending resources that have signed the National Data Privacy Agreement. What is that you ask? Don't worry! We will explain below!

Student Data Privacy Consortium

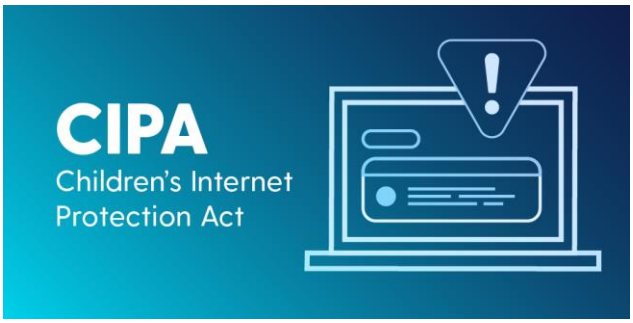
CIPA- Children's Internet Protection Act

Do your students sign a technology agreement each year at the start of the year? If so, this is part of your school's requirements to comply with CIPA.

The purpose of CIPA is to address concerns about children's access to obscene or harmful content that can be found on the Internet. Without getting too detailed, the technology agreement is to address a variety of things including what measures are being taken to prevent minors from accessing harmful materials.

The next aspect of CIPA is in regard to the protection measures put in place by the school/district. Schools and libraries must enforce some sort of filter that blocks and filters internet access on ALL computers. This includes teacher computers!

Lastly, the technology agreement and protection measures must be formally proposed at a public hearing or meeting to be sure it is compliant. Lastly, schools must keep certain documentation to prove their compliance.



FERPA- Family Educational Rights and Privacy Act

Most schools store personal student data in Student Information Systems (SIS). This data might include a student's full name, address, and even social security number.

FERPA requires schools to implement best practices for keeping this data private. It also imposes strict penalties for educational institutes that do not protect their student data. If schools do not comply with FERPA, they could lose their federal funding!

ALL data must be encrypted, which means the data will be protected on a personal device even if it is stolen. Vulnerability scans should take place regularly to find issues within the infrastructure. All systems should be monitored for suspicious activity that might hint at a breach. Finally, compliance standards change, so it is imperative to be aware of these changes.

Some of these best practices may seem outside a typical teacher's comfortability, which is why most districts have an IT department or leader that handles these requirements. However, it is still important for teachers to be *aware* of these protections.

FERPA
Family Educational Rights and Privacy Act

SETIP
Educational Technology Integration Pointers

NDPA- National Data Privacy Agreement

One more acronym to learn, NDPA! This is going to be most helpful for teachers trying to evaluate the safety of websites they use in their classrooms!

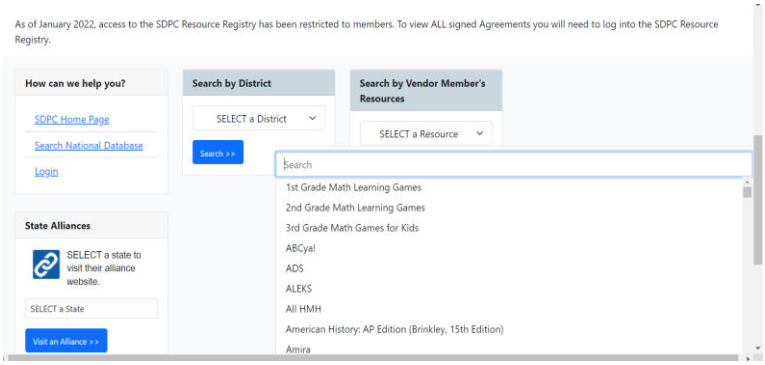
The National Data Privacy Agreement is a contract that educational websites can sign to show they are committed to keeping all student data private! If a website has signed this agreement, they will not sell any student information or data to third parties, they will dispose of student information if requested by the district, they will store all student data within the U.S and provide those locations if requested, they will comply with best practices for keeping data safe, make districts aware if a breach has occurred, along with *many* other safety measures.

Access 4 Learning Community

Student Data Privacy Consortium

So how do you know if a website has signed this agreement? The Student Data Privacy Consortium was formed to help educators identify and use resources that will protect their students. Districts can pay to be a part of this consortium to gain more in-depth information about the NDPAs , but anyone can search the website for information on a resource they would like to use in their classroom.

If your resource is not in the database, check the actual website to see if there is language stating that they have signed a National Data Privacy Agreement. If you do not see this on their website, reach out to the site's support asking that they sign the contract. The contract is easily accessible on the Student Data Privacy Consortium. However, it is probably best practice to involve your school's administration and/or IT department for this process!



Sites that are safe for teacher and student accounts:

Blooket	**Boom Cards**	**Book Creator**
Brainpop	**Canva**	**Code.org**
EdPuzzle	**Flipgrid**	**Google Classroom & Tools**
Gizmos	**IXL**	**Kami**
NewsELA	**Learning A-Z**	**Pear Deck**
SplashLearn	**TinkerCad**	**XtraMath**
Seesaw	**Kahoot**	**iReady**

This list includes a few safe sites, not ALL safe sites!