

# Legislation Overview

## Cybersecurity Regulations in EDU

February 2026

### Overview

In the age of technology, where schools and institutions rely on technology for efficiency and operations, cybersecurity has become an increasingly critical point of concern. If the systems that schools rely on are not properly secured, there is potential for hackers to disrupt the operations and services of institutions across the country. After recent cyberattacks and data mining attempts targeting educational institutions, the federal government has launched several cybersecurity initiatives and regulations. Cybersecurity regulations within education primarily focus on securing and protecting the personal information of students, while ensuring general operations cannot be obstructed.

### Relevant Legislation for EDU:

- **FERPA:** One of the more influential pieces of education-cybersecurity legislation, the Family Rights and Privacy Act ([FERPA](#)) ensures that student education records are secured. This act applies to any institution that receives federal funding, encompassing nearly every institution in the country. One of its primary purposes is to grant parents and students over 18 more control over their educational records. FERPA also prohibits the disclosure of personally identifiable information to outside parties without written consent. The law also grants the government the right to withhold federal funds from any school who consistently violates its principles.
- **PCI DSS:** Higher education institutions must comply with PCI DSS requirements. The Payment Card Industry Data Security Standard ([PCI DSS](#)) is a standard created for credit card companies that regulates the handling of credit card information. When schools and universities receive card payments, they must comply with PCI DSS requirements.
- **NICE Framework for Cybersecurity:** The National Institute of Standards and Technology (NIST) issued a publication ([NIST SP 800-181](#)) which details a framework for cybersecurity work, knowledge and skills. It applies to educators, providing guidance on cybersecurity best practices and the steps required for implementing cybersecurity, supporting education and curriculum

### Relevant Legislation for K-12 ED:

- **COPPA:** The Children's Online Privacy Protection Act ([COPPA](#)) indirectly affects educational institutions. The act is targeted at website and online service providers, prohibiting their collection of personal data for children under 13. It also requires website operators to implement data protection measures as well as restricting data collection and usage. This extends to education technology (EdTech), encouraging K-12 schools to review their third-party service providers compliance with COPPA. Seeing as schools have a responsibility to protect their own student's information through FERPA, it is important for schools to keep compliance in mind when licensing third party solutions.
- **K-12 Cybersecurity Act of 2021:** The K-12 [Cybersecurity Act of 2021](#) focuses on dealing with the increasing threats to cybersecurity within K-12 schools. It mandates that CISA create a report on the cybersecurity risks facing schools and develop recommendations and cybersecurity guidelines based on its findings. This provides schools with a framework for adopting effective cybersecurity practices.
- **CIPA:** The Children's Internet Protection Act ([CIPA](#)) applies to schools and libraries that receive federal funding. It creates regulations requiring schools to implement internet filters, protecting children from obscene content. It also sets forth guidelines on educating children on internet safety practices.

## Relevant Legislation for Higher ED:

**HEOA:** The Higher Education Opportunity Act ([HEOA](#)) contains a cybersecurity component which focuses on protecting student's data as well as combatting copyright infringement. The act implements measures and recommendations for higher education institutions to ensure that students are aware of the consequences of downloading and distributing copyright information. It also provides measures for ensuring the protection of sensitive data.

**GLBA:** The Gramm-Leach-Bliley Act ([GLBA](#)) mandates that financial institutions present their information-sharing procedures to their customers. It also requires financial institutions to defend their customers sensitive data. This applies to colleges and universities, as their large inflow of money classifies them as financial institutions under the GLBA.

**HIPAA:** The Health Insurance Portability and Accountability Act ([HIPAA](#)) contains a component that mandates that all schools must protect their students' insurance and health information. Medical centers located on a school's campus must also be compliant with HIPAA, making this particularly applicable to colleges and universities.

## Relevance to Contractors:

Contractors in the cybersecurity and education space should focus on informing vendors about the legislation. Due to the widespread concern and cybersecurity threats facing education, a significant amount of Federal and State funding will go towards entities that can provide solutions to this issue. Informing vendors of these regulations and guidelines can help them create products that help schools comply with federal cybersecurity regulations. In turn, this will help contractors win awards for cybersecurity in education.

## About Technology by Policy

Tech by Policy is a Carahsoft initiative that helps technology vendors align their solutions to evolving federal, state, and local policy priorities to accelerate growth in the public sector. The program connects policy to procurement—translating executive orders, modernization mandates, and compliance frameworks into actionable go-to-market strategies.

By mapping technology capabilities to government missions, Tech by Policy enables vendors to build visibility, strengthen credibility, and drive adoption through policy-aligned positioning, campaigns, and education.

## Contact Us:

Email:

[Research@carahsoft.com](mailto:Research@carahsoft.com)

### See more from the Carahsoft Team:

To explore our catalog of federal, state, and local technology policies, executive orders, and directives shaping public sector modernization scan this QR code.

