NEW YORK

Student Data Privacy and Security Highlights

New York law and regulations supplement federal privacy protections for for student, teacher, and principal personally identifiable data gathered through the state's professional evaluation system. New York Education Law § 2-d and related regulations such as Part 121 of the Regulations of the Commissioner of Education, which was approved by the Regents in January 2020, provide additional protections for New York students' covered data, including additional data disclosure limitations; establishing reporting requirements and specific consequences for data breaches; and imposing administrative, physical, and technical security requirements.

This section highlights key parts of these state level requirements. However, school districts and other covered entities should consult their local counsel for further information about how to comply fully with these and other important New York requirements.

FERPA FAQs

1. Does New York law and regulation specifically address FERPA's requirements?

SHORT ANSWER: Yes. New York statute requires "educational agencies," which include a school district, board of cooperative educational services, school, or the state education department, to develop and adopt privacy and data security policies that protect student rights consistent with FERPA. Related state regulations expressly adopt FERPA's definitions of "Education Records" and "Personally Identifiable Information."[1] New York law also requires educational agencies to develop and use a Parents' Bill of Rights for Data Privacy and Security, which addresses all student data protections provided by New York and federal privacy laws including FERPA.[2]

DEEPER DIVE: New York law requires every educational agency to develop and adopt a policy on data security and privacy.[3] The law states, "As applied to student data, such policy shall provide all protections afforded to parents and persons in parental relationships, or students where applicable, required under the family educational rights and privacy act, 20 U.S.C. section 1232g [...]."[4] The statute also notes, "The department may only require districts to submit personally identifiable information, including data on disability status and student suspensions, where such release is required by law or otherwise authorized under the family educational rights and privacy act [...]."[5] Each educational agency must also post a Parents' Bill of Rights—the law specifies information that must be included in the document—to its website and include it with every third party contract that involves handling covered personally identifiable student, teacher, or principal data.[6]

2. Does New York law add to federal requirements about data collection and disclosure?

SHORT ANSWER: Yes. New York law prohibits educational agencies from selling personally identifiable information or disclosing it for a commercial or marketing purpose. Educational agencies must also take steps to minimize the collection, processing, or transmission of personally identifiable information.

DEEPER DIVE: New York law requires the Department of Education to use the "least intrusive data collection policies practicable that advance [state education goals] while minimizing the collection and transmission of personally identifiable information."[7] State regulations echo these requirements. Among other obligations under the regulations, educational agencies must ensure that contracts with third parties require that the confidentiality of students, teachers, and principals be maintained consistent with federal and state law as well as the education agency's specific data security and privacy policy.[8]

3. Does New York require data security standards for educational agencies?

SHORT ANSWER: New York law directs the Commissioner of Education, working with the Department of Education's Chief Privacy Officer, to set standards for educational agency data security and privacy policies and develop one or more model policies for their use. The standards must cover data privacy protections and data security protections. As required by the statute, New York's January 2020 education regulations require education agencies to adopt the the National Institute of Standards and Technology (NIST) Cybersecurity Framework by July 2020.

DEEPER DIVE: New York law directs the Commissioner of Education to issue regulations "… establishing standards for educational agency data security and privacy policies and shall develop one or more model policies for use by educational agencies."[9] No later than July 1, 2020, each educational agency—including schools, school districts, BOCES, and other covered educational agencies—must adopt and publish a privacy and data security policy that aligns with the the NIST Framework for Improving Critical Infrastructure, Cybersecurity Version 1.1.[10]

4. Does New York require educational agencies to provide privacy and data security training?

SHORT ANSWER: Yes. Educational agencies must annually provide data privacy and security training to their officers and employees with access to the student, teacher, and principal personally identifiable information covered by the law. Their privacy and security policies must also require training for third party contractors that have access to personally identifiable data.

DEEPER DIVE: New York regulations state," Educational agencies shall annually provide data privacy and security awareness training to their officers and employees with access to personally identifiable information. Such training should include but not be limited to training on the state and federal laws that protect personally identifiable information, and how employees can comply with such laws."[11] The training may be delivered online and may be delivered as part of training the educational agency already offers.[12] Educational agencies must also ensure that their data security and privacy plan specifies how third party contractors and their assignees "will receive training on the federal and state laws governing confidentiality of such data prior to receiving access."[13] If third party contractors violate the statute's data breach notification requirements, the state Department of Education's Chief Privacy Officer can require additional privacy training, among other remedies.[14]

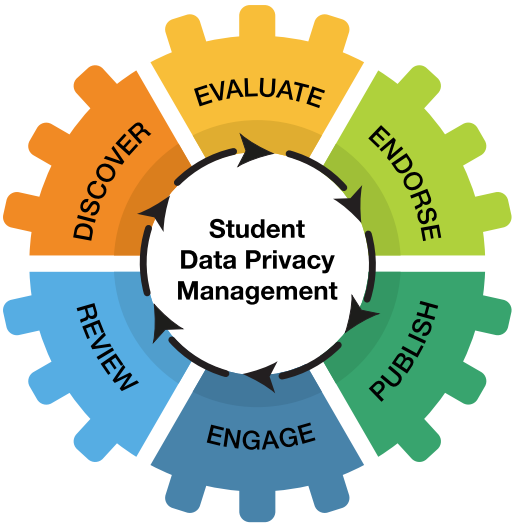
5. Does New York place special data privacy requirements on the third parties that work with educational agencies?

SHORT ANSWER: Yes. New York law states that personally identifiable information maintained by "educational agencies," including data provided to third party contractors and their subcontractors, may not be sold or used for a commercial or marketing purpose.

DEEPER DIVE: Under New York law and regulations, "third party contractors" are "any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency [...]."[15] Additionally, state law says, "Personally identifiable information maintained by educational agencies, including data provided to third-party contractors and their assignees, shall not be sold or used for marketing purposes."[16]

In addition to never selling student, teacher, or principal personally identifiable information or using it for marketing purposes, third party contractors must do the following: "(1) limit internal access to education records to those individuals that are determined to have legitimate educational interests; (2) not use the education records for any other purposes than those explicitly authorized in its contract; (3) except for authorized representatives of the third party contractor to the extent they are carrying out the contract, not disclose any personally identifiable information to any other party" without written consent, unless required by law.[17] Third party contractors must also use reasonable administrative, technical, and physical safeguards (including aligning with the NIST Cybersecurity Framework); encrypt data; honor breach notification requirements; and comply with the data security and privacy policies of the educational agencies with whom they contract.[18]

DEEPER Conversations to Support Student Data Privacy Policy Compliance



DISCOVER new and existing district application usage

EVALUATE application privacy policies, terms of service, and 3rd party policy badging

ENDORSE approved apps by grade, building, or district

PUBLISH list of approved apps, policies, contracts and more with stakeholders

ENGAGE leadership in ongoing conversations on effective usage, results, and application efficacy

REVIEW policy changes, compliance, and application updates

CatchOn allows you to engage your entire leadership team in DEEPER conversations to safeguard your student data and help maintain compliance with state and federal privacy laws.

A few questions your district should consider when selecting a tool to monitor student data privacy compliance:

1. How are you discovering and tracking those apps and online tools your students are using on your school-owned devices that are unknown, not approved, and/or lie outside of your SSO?
2. If you are using an analytics tool to track usage, does that analytics tool allow you to review application information including privacy policies, terms of service, and 3rd party approvals from privacy consortiums like Student Data Privacy Consortium and IMS Global?
3. Does your analytics tool notify you of application policy updates automatically?
4. Are you able to tag your applications for approved use at various grade, building or program level usage?
5. Can you share your application information and privacy policies publicly with district and community stakeholders?
6. Will your analytics tool allow you to see trending application usage within your district, as well as other districts, and monitor accurate application usage by students to the minute with an active window monitoring feature?

CatchOn's Commitment to Promoting Student Data Privacy

CatchOn proudly supports and has signed the Student Privacy Pledge. As a software as a service solution that is both a software discovery and usage tracking tool for applications, CatchOn is committed to protecting student data. Our 360-degree approach to student data privacy helps you keep your data safe and provides you real-time visibility into the learning tools being used in your school district.

See how CatchOn specifically helps districts stay compliant with education privacy laws below.

Education Law What is Required at a Glance	**CatchOn's Solution** How CatchOn Can Help You Stay Compliant	
Review 3rd party agreements	Affords quick access to 3rd party websites and privacy policies	✓
Ensure District privacy/security policies are aligned	Provides ability to mark and categorize applications as approved or not approved by the district	✓
District data protection office	Enables education leaders to see software applications used on school devices, both inside and outside the classroom; Empowers leaders to diagnose applications vulnerable to student data privacy policies	✓
Continuous review for compliance	Provides the ability to monitor known and unknown apps for compliance	✓
Parental notifications	Enables districts to post and share approved and monitored apps with parents using automated reports	✓
Breach notification plan	Provides the ability to gather data on EdTech usage, applications privacy policies, and district purchases to avoid vulnerabilities	✓
Align to NIST framework and FERPA policies	CatchOn tracks only de-identified aggregated information PII stays on district server; CatchOn signed student privacy pledge	✓
Privacy training	Enables districts to facilitate training opportunities by leveraging data analytics that track data usage, trends, and impact	✓

[1] 8 NYCRR Part 121.1.
[2] NY EDN Law 2-d, Sec 3. Parents Bill of Rights for Data Privacy and Security.
[3] NY EDN Law 2-d, Sec. 5. Data Security and Privacy Standards.
[4] Ibid.
[5] NY EDN Law 2-d, Sec. 4. Data Collection Transparency and Restrictions.
[6] NY EDN Law 2-d, Sec. 3. Parents Bill of Rights for Data Privacy and Security.
[7] NY EDN Law 2-d, Sec. 4. Data Collection Transparency and Restrictions.
[8] 8 NYCRR Part 121.2.
[9] NY EDN Law 2-d, Sec. 5. Data Security and Privacy Standards.
[10] 8 NYCRR Part 121.5.
[11] 8NYCRR Part 121.7.
[12] Ibid.
[13] 8 NYCRR Part 121.6.
[14] 8 NYCRR Part 121.11(e)(4).
[15] NY EDN Law 2-d, Sec. 1. Definitions.
[16] NY EDN Law 2-d, Sec. 4. Data Collection Transparency and Restrictions.
[17] NY EDN Law 2-d, Sec. 5. Data Security and Privacy Standards.
[18] Ibid. See also 8 NYCRR Part 121.9.

Provided by:

An ENA Affiliate
catchon®

CatchOn is an expansive data analytics tool that compiles real-time data on every device, enabling school districts to make data-informed decisions about the apps and online tools their educators and students are using. In 2018, CatchOn joined forces with ENA, a leading provider of comprehensive technology solutions to education institutions and libraries across the nation. Collectively, CatchOn and ENA leverage their respective resources and expertise to deliver critical services and solutions that help school districts produce positive outcomes in the communities they serve. For more information, please visit www.catchon.com, call **866-615-1101**, or email **solutions@catchon.com**

FORESIGHT LAW+POLICY

Foresight Law + Policy is a national education law firm based in Washington, D.C. Our lawyers and other professionals counsel education leaders, nonprofit organizations and companies working to strengthen public education and prepare all kids for success. For more information, please visit https://www.flpadvisors.com/

Contributing Author:
Reg Leichty, Founding Partner

SETDA
LEADERSHIP • TECHNOLOGY • INNOVATION • LEARNING

Founded in 2001, the **State Educational Technology Directors Association (SETDA)** is the principal nonprofit membership association representing US state and territorial educational technology leaders. Our mission is to build and increase the capacity of state and national leaders to improve education through technology policy and practice. For more information, please visit setda.org.