NEW HAMPSHIRE

Student Data Privacy and Security Highlights

New Hampshire laws and regulations supplement FERPA's access and disclosure requirements for education records. New Hampshire does not report individual student level data, and all management of education records must be in compliance with all applicable laws, including FERPA and a number of state laws. Like FERPA, New Hampshire's education statute expressly prohibits, with limited exceptions, schools from disclosing personally identifiable information without consent while also providing the student's parents and eligible students the right to access their records.

This section highlights key New Hampshire protections for student data but does not provide a comprehensive list of statutory and regulatory requirements. Readers should consult their local counsel for further information about New Hampshire law.

FERPA FAQs

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

SHORT ANSWER: New Hampshire statute specifies that the Department of Education, as well as each local education agency, is required to manage student records in compliance with FERPA and all applicable state laws.

DEEPER DIVE: New Hampshire's statute states that the New Hampshire Department of Education and each local education agency must "make publicly available students' and parents' rights under the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. section 1232g, et seq., and applicable state law."[1] This includes the right to provide "written consent before the school discloses student personally identifiable data from the student's education records, provided in applicable state and federal law."

New Hampshire statutes limit the release of pupil names or codes in statewide assessment results, scores, or other evaluative materials; however, individual pupil results will be "made available to a parent, a legal guardian, or the pupil's school in accordance with the Family Educational and Privacy Rights Act, 20 U.S.C. 1232g."[2]

2. Does New Hampshire law limit access to personally identifiable student records?

SHORT ANSWER: Like FERPA, New Hampshire law limits access to personally identifiable student records and prohibits the state from allowing personally identifiable information to be connected with a "unique pupil identifier" while also providing a list of statutory exceptions to the consent requirement.

DEEPER DIVE: New Hampshire's Student and Teacher Information and Protection and Privacy Act requires school districts to provide notice of students' and parents' rights under FERPA, including the right to provide "written consent before the school discloses student personally identifiable data."[3]

Regarding state-level student data, New Hampshire law requires the Department of Education to maintain a "unique pupil identification system," which is an electronic system comprised of a data warehouse and a random number generator or "unique pupil identifier."[4] The data warehouse is an electronic system operated by the Department of Education; however, it may not contain the "name, address, telephone number, e-mail address, social security number, or any other personally identifiable information about any pupil." The pupil identification system limits access to the information contained within. New Hampshire law states that "no personally identifiable information about a pupil including name and social security number, shall be collected or maintained by the state as to allow such information to be connected with the unique pupil identifier."[5] This statute states that access to unique pupil identifiers and data, absent a court order, is limited to the following: (1) a parent, legal guardian, or foster parent; (2) the student, if the student is 18 years of age or older; and (3) early childhood program directors or designees, district superintendents or designees, and postsecondary institutional registrars or designees if the pupil is pursuing education in such programs. Further, the Department of Education may grant access to the data warehouse where all of the information is stored if access is needed to connect information in the warehouse with the random number generator.

Pupil assessment results may be made available to parents, legal guardians, or the pupil's school so long as the release of information is in accordance with FERPA.[6]

3. Does New Hampshire place restrictions on FERPA's "directory information" exception?

SHORT ANSWER: No. New Hampshire requires local education agencies to comply with FERPA's directory information exception with no additional restrictions.

DEEPER DIVE: New Hampshire law states that a "local education agency which maintains education records may provide information designated as directory information consistent with the Family Educational Rights and Privacy Act (FERPA)."[7] Parents must be given public notice of the information that is considered "directory information" and parents must submit a written request to remove their student's information if they do not wish for that information to be available to the public, which shall be done on an annual basis. The items that are considered "directory information" include the following: (1) name and address; (2) field of study; (3) weight and height of athletes; (4) most recent previous school attended; (5) date and place of birth; (6) participation in officially recognized activities and sports; and (7) date of attendance, degrees, and awards.

4. Does New Hampshire provide a model data security plan for school districts?

SHORT ANSWER: No; however, the New Hampshire Department of Education has released the Minimum Standards for Privacy and Security of Student and Employee Data, which defines minimum requirements for guarding student and employee information, for local education agencies. Further, the Department of Education launched The Initiative for School Empowerment and Excellence (i4see) that provides guidance and support regarding the collection of student data.

DEEPER DIVE: New Hampshire statute requires the Department of Education to establish "minimum standards for privacy and security of student and employee data, based on best practices, for local education agencies."[8] According to the Minimum Standards for Privacy and Security of Student and Employee Data, all local education agencies must implement these standards. These minimum standards establish the "minimally acceptable baseline of security and privacy." According to the New Hampshire Department of Education's frequently asked questions, the minimum standards complement FERPA.

The Initiative for School Empowerment and Excellence (i4see) is a student level data collection and seeks to reduce the burden on districts, improve the quality of data, and allow for important analysis of student data. Among other deliverables focused on student data privacy, this initiative provides support guides, tip documents, and policy and procedure manuals.

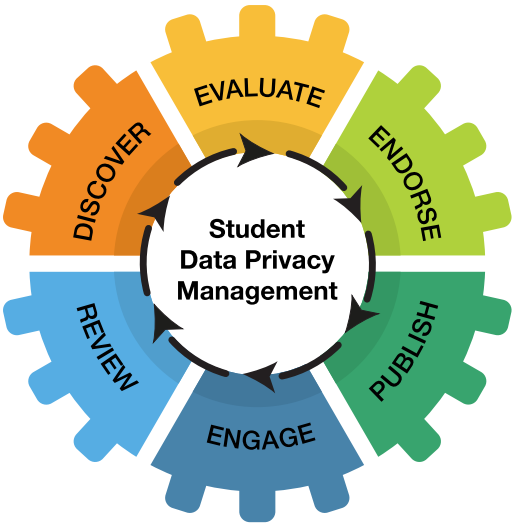
5. Does New Hampshire place special data privacy requirements on the third parties that work with schools and the state department of education?

SHORT ANSWER: The department of education is subject to data disclosure limitations. New Hampshire law prohibits "operators" from selling a student's personally identifiable information, using it for targeted advertising, or amassing student profiles. The law also requires operators to meet other specific privacy requirements.

DEEPER DIVE: New Hampshire prohibits the department of education from providing student personally identifiable data for any purpose to a "public or private individual or entity, including the local, state, or federal government, or department or agency thereof, regardless of whether such individual or entity is for profit or not-for-profit, and regardless of whether the public or private individual or entity is involved in any way with the pupil's education." However, if there is authorization provided by statute, the department may provide such information.[9] New Hampshire provides some exceptions for testing companies so long as the information is only used to identify the test taker and certain specific requirements are met.[10]

New Hampshire law also places limits on "operators" who access student online personal information.[11] "Operators" are defined as an "operator of an Internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K-12 school purposes and was designed and marketed for K-12 school purposes." Operators are prohibited from knowingly engaging in targeted advertising, using information to amass a profile about a K-12 student, selling student information including covered information, and disclosing information unless the disclosure is made to respond to or participate in a judicial process. Any operator is also required to implement and maintain "reasonable security procedures and practices" and delete information when requested. Operators are allowed to use student information under certain limited circumstances, including the use of deidentified information to improve educational products or demonstrate the effectiveness of products or services, including in marketing. Internet service providers may use information to provide Internet connectivity to schools or students and their families, among several other exceptions.

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] NH RSA 189:66
[2] NH RSA 193-C:11.
[3] NH RSA 189:66.
[4] NH RSA 193-E:4.
[5] NH RSA 193-E:5.
[6] NH RSA 193-C:12.
[7] NH RSA 189:1-e.
[8] NH RSA 189:66.
[9] NH RSA 193-E:5.
[10] NH RSA 189:67.
[11] NH RSA 189:68-a.

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.