VIRGINIA

Student Data Privacy and Security Highlights

Virginia laws and regulations reflect and supplement FERPA's access and disclosure requirements for education records, which the state interchangeably refers to as "scholastic records." Virginia State Board of Education regulations require school districts to manage scholastic records of all students in compliance with all applicable laws, including FERPA, the federal Individuals with Disabilities Education Act, and a number of state laws. Like FERPA, Virginia's education statute expressly prohibits schools from disclosing personally identifiable information without consent while also providing parents and eligible students the right to access their own records, except in very limited circumstances.[1]

This section highlights key Virginia 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 Virginia law.

FERPA FAQs

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

SHORT ANSWER: Virginia statute and Virginia education laws direct school districts to manage student records in compliance with FERPA and all applicable federal and state laws.

DEEPER DIVE: Virginia's statute requires the Department of Education to make policies to "ensure state and local compliance with the Family Educational Rights and Privacy Act (20 U.S.C.§1232g) and related regulations." Virginia's Administrative Code (State Board of Education Regulations) requires school districts to "manage the scholastic records of all students in compliance with applicable law, including the Family Educational Rights and Privacy Act" as well as state law applicable to students' personally identifiable information.[2] Other federal privacy requirements referenced in this section of state regulations include the privacy provisions and related regulations of the Individuals with Disabilities Education Act.

2. Virginia law uses the term "scholastic record," but FERPA uses the term "education record". Do these definitions refer to the same student data?

SHORT ANSWER: Yes. Virginia Department of Education guidance states that the terms "education record" and "scholastic record" may be used interchangeably.[3]

DEEPER DIVE: Virginia law states that a "scholastic record" means "those records that are directly related to a student" and are maintained by a a school district, school, or party acting for them. Such records may be "recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche." [4] Virginia Department of Education guidance published in 2004 states that the term "education record" is used in FERPA whereas "scholastic record" is used in the Code of Virginia.

3. Does Virginia law limit access to personally identifiable student records?

SHORT ANSWER: Like FERPA, Virginia law places a general restriction on school employees and school board members from disclosing personally identifiable student records without parent or eligible student consent, while also providing a list of statutory exceptions to the consent requirement.

DEEPER DIVE: Virginia State Board of Education regulations state that scholastic records shall be managed in compliance with applicable law, including FERPA as well as state statutes including requirements in Virginia applicable to "pupil records."[5] Virginia law says "[n]o teacher, principal or employee of any public school nor any school board member shall permit access to any records concerning any pupil [...] except under a judicial process" to the following people: (1) the pupil's parents or to the pupil if they are age 18 or older; (2) "[a] person designated in writing" by a pupil age 18 or older or by the parent of a pupil less than 18 years of age; (3) a principal, or his or her designee, of a school the pupil attends, has attended, or intends to enroll; (4) "current teachers" of the student; (5) state or local law enforcement seeking information in the course of their duties; (6) the superintendent or superintendent staff member where the pupil attends, has attended, or intends to enroll; or (7) a city or county agency responsible for protective services to children when a minor is referred for services.[6]

4. Does Virginia place restrictions on FERPA's "directory information" exception?

SHORT ANSWER: Virginia schools should not use the FERPA directory information exception to disclose a student's address, phone number, or email address.

DEEPER DIVE: Virginia law narrows the use of FERPA's directory information exception. Under state law, a school may not use the directory information exception to disclose the address, phone number, or email address of a student unless the parent or eligible student has affirmatively consented in writing to such disclosure. This does not prohibit disclosing a student's address, phone number, or email address to students enrolled in the school or school board employees for educational purposes or school business so long as the parent or eligible student has not opted out of such a disclosure.[7]

5. Does Virginia provide a model data security plan for school divisions?

SHORT ANSWER: The Virginia Department of Education (VDE) is required to work with the Virginia Information Technologies Agency to provide a model data security plan. VDE elected to meet this statutory obligation by joining the Access 4 Learning Community, which offers school divisions access to a range of data security and privacy resources.[8]

DEEPER DIVE: Virginia law requires the Department of Education to "develop, in collaboration with the Virginia Information Technologies Agency, and update regularly but in no case less than annually, a model data security plan for the protection of student data held by school divisions. Such model plan shall include (i) guidelines for access to student data and student data systems, including guidelines for authentication of authorized access; (ii) privacy compliance standards; (iii) privacy and security audits; (iv) procedures to follow in the event of a breach of student data; and (v) data retention and disposition policies. The model plan and any updates shall be made available to every school division."[9] As described above, VDE elected to provide school divisions this required information by joining the Access 4 Learning Community.

6. Does Virginia place special data privacy requirements on the third parties that work with schools?

SHORT ANSWER: Yes. Virginia law prohibits "school service providers," such as a website, mobile application, or online service that collects, uses, or maintains personally identifiable student data, from selling the data or using it for targeted advertising. The law also requires school service providers to meet other specific privacy requirements.[10]

DEEPER DIVE: Under Virginia law, "school service providers" are entities that "operate a website, mobile application, or online service that (i) is designed and marketed solely for use in elementary or secondary schools, (ii) is used at the direction of teachers or other employees at elementary or secondary schools, and (iii) collects and maintains, uses, or shares information that identifies an individual student or is linked to information that identifies an individual student to maintain certain protections for such information, including transparency, privacy policies, information security programs, and access to an individual student's personal information by the student and his parents."[11]

In addition to never selling student personal information or using it for targeted advertising, school service providers must do the following: publish information about the information they collect and how it is maintained, used, or shared; adopt and follow a privacy policy and provide notice of it; maintain a comprehensive information security program; facilitate access to and correction of student personal information in its possession; satisfy consent requirements; require successor entities to satisfy the requirements; and delete information at the request of the school or school division.[12]

DEEPER Conversations to Support Student Data Privacy Policy Compliance
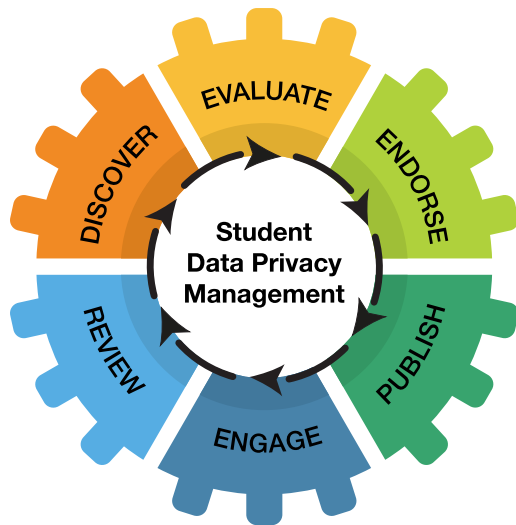
DISCOVER new and existing district application usage

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] Virginia Code § 22.1-287(B); Virginia Administrative Code 20-150-20 Management of Scholastic Record.

[2] Virginia Administrative Code, 20-150-20 Management of Scholastic Record.

[3] Guidelines for The Management of the Student's Scholastic Record in The Public Schools Of Virginia, Virginia Department of Education (2004), available online at http://bit.ly/2uGpbk3.

[4] Virginia Code § 22.1-289(A).

[5] Virginia Administrative Code, 20-150-20 Management of Scholastic Record.

[6] Virginia Code § 22.1-287(A)(1-7).

[7] Virginia Code § 22.1-287.1. Directory Information.

[8] James F. Lane, Ed.D., Superintendent of Public Instruction Memo to Division Superintendents re Student Data Privacy Resources, Superintendent's Memo # 073-19, April 5, 2019.

[9] Virginia Code § 22.1-20.2. Student data security.

[10] Virginia Code § 22.1-289.01.

[11] Virginia Code § 22.1-289.01(A).

[12] Virginia Code § 22.1-289.01(B) and (C).

Provided by:

An ENA Affiliate
Catch On ®

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.