

SB1486

Public schools; protection of student records and personal information, policies and procedures.



Bill Patron: Senator Luther Henry Cifers, III (10th Senate District)

What The Bill Does:

Establishes certain enumerated requirements for the protection of student personal information on school-issued devices, as defined in the bill, by public schools, school boards, and by school technology providers, as defined in the bill. "*Student personal information*" means information collected through a school service that identifies a currently or formerly enrolled individual student or is linked to information that identifies a currently or formerly enrolled individual student.

Upon request, the school division would have to provide access to an electronic copy of such student's personal information in a manner consistent with the functionality of the school service or school-issued device to the parent or eligible student. The bill requires that all school-issued devices that a student returns have all student personal information stored in the school-issued device deleted within a reasonable time after such school-issued device is returned to the division and prior to the subsequent provision of such school-issued device to any other student or other transfer in ownership of such school-issued device.

The legislation prohibits schools from knowingly sharing student personal information for the purpose of targeting advertising to students; sharing student personal information to create a personal profile of student; as well as use any school-issued device to access or monitor (i) location-tracking features; (ii) audio or visual receiving, transmitting, or recording features; or (iii) student interactions, unless such use (a) is limited to a noncommercial, educational, or instructional purpose, to the provision of technical support, or to exam proctoring by a school board employee or a third party pursuant to a contract with the school board and notice of such use is provided in advance or (b) is permitted under a judicial warrant or is necessary to comply with state or federal law.

The bill provides that nothing in the Code section shall be construed to prohibit any school board from requesting or prohibit any provider from granting any school board access to or the ability to monitor school-issued devices to ensure compliance with a school code of conduct or otherwise limit the ability of any school board to use software filters to monitor school-issued devices for certain safety threats, self-harm prevention, or other risk indicators.

Why Does This Matter?

This bill strengthens the requirements of school divisions in the protection of student personal information as rigorously as data handled by third-party education platforms covering everything from privacy policies and breach notifications to prohibiting targeted ads or non-school-authorized tracking. With the growing landscape of EdTech products and tools used in schools, this will further protect student privacy and ensures consistent, statewide safeguards for students' personal information whenever they use division-provided technology and devices.

How Does This Impact Students?

SB1486 ensures that every public school student using school-issued technology enjoys standardized, robust privacy measures safeguarding their personal information. Schools must now treat student personal information on devices with the same level of care as they do for third-party education platforms, ensuring data is not misused or exposed. With mandatory protections in place, students using school-issued laptops, tablets, or other digital tools can have greater confidence that their privacy is respected and sensitive data is shielded from unauthorized access.

How Does This Impact School Divisions?

- School divisions are required to delete any student personal information stored in the school-issued device within a reasonable time after such school-issued device is returned and prior to the subsequent provision of such school-issued device to any other student or other transfer in ownership of such school-issued device.
- School divisions shall collect, maintain, use, and share student personal information only with the consent of the student or, if the student is less than 18 years of age, his parent or for the purposes authorized in the contract between the school division and the school service provider or school technology provider.
- School divisions will need to facilitate receiving parental consent for those uses stated.
- Schools will have to ensure that any school technology providers that they do business with comply with the provisions of the legislation.
- Nothing prohibits any school board from requesting or prohibit any provider from granting any school board access to or the ability to monitor school-issued devices to ensure compliance with a school code of conduct or otherwise limit the ability of any school board to use software filters to monitor school-issued devices for certain safety threats, self-harm prevention, or other risk indicators.

What Resources Are Available?

- VDOE provides all Virginia school divisions with the opportunity to be a part of the [Student Data Privacy Consortium](#), which is managed by a nationwide nonprofit known as “a41.” The Consortium provides Virginia school divisions with the benefit of a negotiated and approved Virginia student data privacy agreement that can be used with Educational Technology school technology providers by exercising an additional addendum that allows a school division to sign onto an agreement that has been executed by another Virginia School division.

What Additional Items Will Be Released?

- In addition to this one pager, notice of this legislation will be provided in a Virginia Education Update newsletter article prior to August 1, 2025.

School Division Next Steps:

1. Schools are required to provide parents with information about the specific personal data that is collected about their student and how it maintains, uses, or shares such student personal information.
2. When requested, schools must provide parents with access to an electronic copy of such student's personal information in a manner consistent with the functionality of the school service or school-issued device.
3. Schools must delete student personal information on a school issued device when it is turned in to be sold or repurposed. **This should already be being done, but this law will require it.**
4. School technology providers are permitted to access or monitor school-issued devices, if monitoring is limited to a noncommercial, educational, or instructional purpose, to the provision of technical support, or to exam proctoring by a school board employee or a third party pursuant to a contract with the school board and notice of such use is provided in advance or is permitted under a judicial warrant or is necessary to comply with state or federal law.

Who is the VDOE Contact:

Paul Cormal, Assistant Superintendent for Data, Research and Technology

Paul.Cormal@doe.virginia.gov

804-839-9653

If interested in joining the Student Data Privacy Consortium, contact:

Diane Carnohan, Chief Information Security Officer

Diane.Carnohan@doe.virginia.gov

804-659-3309