Policy: 02 - Legal Alert
Section: Special Release - October 2024

Special Release - October 2024 - New Senate Bill 29 Limits School Monitoring of Student Devices and Accounts, Places Requirements on Third Party Vendor Contracts

LEGAL ALERT

To: Neola Clients

From: Ennis Britton Co., LPA

Re: Senate Bill 29 Limits School Monitoring of Student Devices and Accounts, Places Requirements on Third Party Vendor Contracts

Date: October 2024

The Ohio General Assembly passed Senate Bill 29 at the end of June 2024, and it was signed by the Governor in July. The bill was passed amidst a growing global focus and concern about personal data mining and data privacy. SB 29 was drafted to enhance student data privacy in particular. However, in doing so, the law places a significant number of new responsibilities on public school districts which might prove challenging to fulfill. The law takes effect October 24, 2024[1], although some provisions do not require immediate action as described below.

SB 29 modifies two (2) existing statutes which govern public records and educator licensure, and enacts three (3) new statutes – R.C. 3319.325, 3319.326, and 3319.327. Several other State and Federal laws which protect the use and privacy of student education records remain in full effect, and should be taken into consideration as districts implement SB 29 changes. One of these laws is the Family Educational Rights and Privacy Act ("FERPA").[2] FERPA defines student education records broadly to include records that are 1) directly related to a student; and 2) maintained by an

educational agency or institution or by a party acting for the agency or institution. There are several important exceptions to this definition under FERPA, including: 1) records that are kept in the sole possession of the creator that are used as a memory aid and not shared with any other person except a temporary substitute for the record creator; 2) employee personnel records; 3) certain law enforcement records; and 4) medical treatment records for students who are over the age of eighteen (18).

State law, specifically R.C. §3319.321, also governs confidentiality of student records and personally identifiable student information. This law is arguably even more restrictive than FERPA, and broadly prohibits an individual from releasing or permitting access to personally identifiable student information other than directory information without written parent consent.

The following summarizes the four (4) main sections of SB 29.

Part One: Public Records Exemption for "Educational Support Services Data"

SB 29 modified the Ohio Public Records Act, R.C. §149.43, to add a new category of records, specifically "educational support services data," that are not considered public records and therefore are not subject to release. "Educational support services data" is defined in R.C. §3319.325 as:

". . . data on individuals collected, created, maintained, used or disseminated relating to programs administered by a school district board of education or an entity under contract with a school district designed to eliminate disparities and advance equities in educational achievement for youth by coordinating services available to participants, regardless of the youth's involvement with other government services."

This change is focused not on education records as a whole, but more narrowly on the data that a school district creates and maintains related to services provided to students that are designed to increase equity and educational achievement. SB 29 requires that districts make this data available to the Opportunities for Ohioans with Disabilities ("OOD"), a State agency that is publicly funded with a goal to help individuals with disabilities achieve employment and independent living. The law declares that schools must still provide OOD with records that support their activities.

This provision takes effect October 24th, 2024.

***Action Steps for Part One**:* Staff who assist the district in responding to public records requests should be made aware of this new public records exemption. If an individual who is not requesting records on behalf of OOD submits a public records request for these records, the request should be denied and the new provision of the law should be cited as the basis for the denial. The specific citation is R.C. §149.43(A)(1)(tt).

Part 2: Licensure Action for Breaches of Confidentiality

SB 29 expressly authorizes the State Board of Education to reject a license application or suspend, revoke, or limit the license of an individual who uses or releases information that is deemed confidential under State or Federal law concerning a student or a student's family members for any purpose other than student instruction.

As mentioned previously, school districts are already subject to stringent legal requirements governing the use of student education records. Interestingly, the State Board's *Licensure Code of Professional Conduct for Ohio Educators* also addresses confidentiality in very broad terms. One of the nine rules is dedicated to the topic and includes language that is similar to what now appears in amended R.C. §3319.31. The SB 29 change now places this restriction directly in State law.

This section of SB 29 takes effect October 24th.

Action Steps for Part Two: This provision impacts the State Board of Education more directly than a district. However, if you have not recently reminded licensed staff members about their obligation to comply with State and Federal confidentiality laws, now might be a good time. Staff need to

understand that they risk not only possible discipline from their school employer but also adverse action against their State-issued license when they violate confidentiality. They should be diligent in making sure that communications about students and their family members remain professional and confidential at all times.

Part Three: New Requirements for a District's Technology Providers

The most significant changes to be enacted in SB 29 came from the adoption of three (3) new statutes: R.C. Sections 3319.325, 3319.326, and 3319.327. This trio is keenly focused on student privacy and places new restrictions and expectations on district contracts with technology providers as well as on how the technology providers may access and use student data.

For the purpose of these statutes, SB 29 adopts some key definitions that are important to know about as your district prepares to implement the law. Three (3) definitions are particularly important as we examine the new requirements for technology providers.

For instance, the term "educational records" is defined to include "records, files, documents, and other materials that contain information directly related to a student and are maintained by a school district board of education *or by a person acting for the school district."* The definition excludes records created by educational personnel that are maintained in their sole possession, records made and maintained by the school during the normal course of business that relate to an employee and not available for any other use (i.e. employee personnel records), and records generated by certain medical providers while providing treatment to students over the age of eighteen (18). These exceptions generally align with ones included in FERPA, but with a few interesting deviations.

For instance, the "sole possession" exception under the new State law applies specifically to "records of **instructional**, **supervisory,** and **administrative personnel**, and **educational personnel**". FERPA's exception applies more broadly to records in the sole possession of any "maker", without specifying any roles that the maker has in the district. Likewise, the revised State law indicates that the records may be shared "with **substitute teachers**", where the Federal law declares they may be shared with anyone who serves as "a substitute for the maker." While these might seem like relatively minor differences, they may prove more relevant over time as the new law takes effect and Ohio schools attempt to implement it.

The drafters were also very specific about which "technology providers" they wanted included under the new laws. The definition encompasses any person (and presumably any entity) "who **contracts with** a school district **to provide a school-issued device** for student use **and creates, receives, or maintains educational records** pursuant or incidental to its contract with the district." The definition appears to attach the new requirements to only those technology providers who have a contract with the district to provide devices.

The term "school-issued device" is important here as well, because it helps a district to identify which technology providers are subject to the new rules. The term is defined somewhat strangely to include all "**hardware, software, devices, and accounts** that a school district, acting independently or with a technology provider, **provides to an individual student** for that **student's dedicated personal use.**" This definition is much broader than what the term "device" might imply. It also covers student accounts that are issued by school districts.

Certain language is highlighted in these definitions for a reason. We know that when a law is drafted, the words that legislators use really matter. Sometimes those words have unintended consequences, which may prove to be the real challenge with this bill. As educators, attorneys and other stakeholders review and contemplate the meaning and implications of the various provisions, there seem to be more questions than answers about what the legislators actually meant and expect from schools. Recently, some members of the General Assembly have voiced a willingness to consider revisions, which will hopefully help clarify expectations. In the meantime, school districts should pay attention to these definitions as you plan to implement the following new requirements:

A. ***Technology Providers Must Now Comply with Chapter 1347 and Disclose Certain Information when There is a Breach***

Under the new law, a third-party technology provider must now comply with the same laws that school districts and other public entities follow under Chapter 1347 "as if it were a school district." Chapter 1347, which is often referred to as the Ohio Personal Information Systems Act or Ohio Privacy Act, was originally drafted to regulate the collection, use, and protection of data used by State and local government agencies that maintain personal information systems. It includes provisions that govern the use of personal information, personal rights of individuals whose information is maintained in the systems, disputes about the accuracy of the data, **disclosure of data breaches,** and more. Private technology providers that were previously not governed by these rules will need to comply with them in order to do business with public schools in Ohio moving forward.

As for data breaches in particular, the new law mandates that in the event educational records that are maintained by a technology provider are subject to a breach of the security of the data as defined by R.C. §1347.12, the technology provider must upon discovering the breach disclose all the information to the school district that it needs to fulfill the notice requirements of Chapter 1347.

R.C. 1347.12 is triggered when there is unauthorized access of personal information contained in a government system (and now, thanks to SB 29, the system of a technology provider doing business with the school). "Personal information" specifically references the data that someone might use to steal a person's identity. This includes an individual's first name or first initial and last name that is accessed in combination with or linked to their social security number, driver's license or State identification card, account number or credit/debit card number combined with the password that is needed to access the account.

Once a school district or other public entity becomes aware of a breach of personal information, it is required under R.C. 1347.12 to notify any State resident whose personal information may have been compromised by the breach if such access may reasonably be believed to present a risk of identity theft. The notice should be sent "in the most expedient time possible" but no later than forty-five (45) days following its discovery. Since this law attaches a specific timeframe, prompt notice of a breach by a technology provider is key. It is also critical that the technology provider relays all the information that the district might need to send the required notice.

B. *Records are Sole Property of School Districts*

The new law also unequivocally declares that any educational records created, received, maintained, or disseminated by a technology provider as they fulfill the terms of a service contract with a district remain the sole property of the district, and must be returned or destroyed within ninety (90) days after the expiration of the contract unless a renewal of the contract is reasonably anticipated. Moving forward, districts may want to include contract provisions which address this requirement, if they are not already in the current contract. Some contracts may already require the destruction or return of records, but may permit a longer period of time to do so. These provisions should be updated as well to align with this new requirement.

C. *Technology Provider Limits on Use of Student Data*

Technology providers are prohibited from selling, sharing or disseminating educational records except as provided by the new statute unless the action has been delegated or assigned to another entity through the service contract with the district.

Technology providers may not use educational records for any commercial purposes, including marketing or advertising to students or their parents/guardians. However, providers may use aggregate data that has been stripped of personally identifiable information for improvement, maintenance, development, support, or diagnosis of the provider's site, services, or operations.

D. *Requirements for Technology Provider Contracts*

Contracts between tech providers and school districts must now include a provision that ensures appropriate security safeguards are in place to protect educational records, including restrictions on unauthorized access

by employees or contractors. Employees and contractors are authorized to access records only when necessary for them to fulfill their official duties.

E. ***CAT Technology Provider Annual Notice to Parents***

Beginning in the 2025-2026 school year, annually by August 1st districts are required to provide "direct and timely notice" by mail, email or other direct means to parents and students that lists any **curriculum**, **assessment** or **testing** ("CAT") technology provider **contract** affecting a student's educational records.

Note that the use of the terms highlighted here appear to narrow this requirement to only those technology provider contracts that involve curriculum, assessment or testing **and** "affects" a student's educational records. The language has certainly caused confusion. Some districts plan to take a conservative approach and list all technology provider contracts in their notice. Others might choose to take a narrower view of which contracts must be captured in the notice. It is recommended that you contact legal counsel to discuss this further.

The notice a district provides must specifically:

1. identify each curriculum, testing, or assessment technology provider with access to educational records;

2. identify all educational records affected by the curriculum, testing or assessment technology provider contract;

3. include information about how parents may inspect technology provider contracts; and

4. list who parents may contact in the district for more information or to express concerns.

Creating a notice that covers all of these providers and contains the required data elements may prove to be a challenge. Since August 1 has already come and gone for this school year and the law is not yet in effect, districts have time to gather all the required elements of the notice for next year.

F. ***Inspection of Technology Provider Contracts***

Schools are also required by SB 29 to provide parents and students with an opportunity to inspect a complete copy of each technology provider contract. Because these contracts are typically public records, it is reasonable to treat requests to inspect contracts in the same way you handle other public records requests. The statute provides that parents and students have a right to inspect contracts, not necessarily to receive copies. That said, it is often easier to send electronic copies if a request is made. Districts should be consistent in how they respond to these requests. Any redactions required by law should still be made. Districts may also elect to post the contracts in a central location or provide links to the contracts in their electronic notice.

Action Steps for Part Three: Identifying and managing technology use is key. It is important to work with your information technology staff and administrators to identify the technology providers that might be covered under the new law. These providers should be notified about the recent changes so that they can prepare to implement the new requirements.

Contracts with technology providers should also be located and ideally stored in a central location that is accessible to key staff. While changes may not need to be made to contracts that are in effect at the time the new law takes effect, these contracts should be carefully reviewed by administration and legal counsel to ensure compliance as they expire and new contracts are entered into.

This law should also prompt ongoing investment in ensuring that staff only use the technology platforms approved by the district's IT staff or central office administrators and that staff follow a

formal approval process before using new technology. While educators may wish to start using the latest apps and software as soon as they hit the market, due to the contract requirements on use of data, it is essential that a formal procedure is in place. Districts should make sure staff are well informed of the new requirements student data privacy and use of technology providers.

Finally, districts should begin to compile information needed to draft a notice and develop a process so that notices are ready to be sent by August 1, 2025.

Part Four: Access and Monitoring Restrictions for Student Activities on Devices

Last, but certainly not least, SB 29 includes a new provision that restricts a district's ability to access or monitor student activities on school-issued devices and accounts. The law generally forbids a district from monitoring or accessing the following:

A. location tracking features on school-issued devices;

B. audio/visual receiving, transmitting, or recording features on such devices; and

C. data about student interactions with a school-issued device, including but not limited to keystrokes and web browsing. for limited exceptions.

However, there are several limited exceptions. These restrictions do not apply in the following circumstances:

A. Activities of school employees, student teachers, and third-party contractors or vendors that are limited to a noncommercial educational purpose for instruction, technical support, or exam proctoring, **provided that notice is given in advance**.

B. Activities that are performed to comply with a judicial warrant.

C. Activities on technology performed to help recover devices upon receiving notice that the device is missing or has been stolen.

D. Activities necessary to prevent or respond to a threat to life or safety, **provided that access is limited to that purpose**.

E. Activities that are necessary to comply with State or Federal law; and

F. Activities that are necessary to participate in a State or Federal funding program such as E-Rate.[3]

This provision of the law includes two (2) additional notice requirements:

A. **Requirement to Provide General Notice.** If a district plans to engage in any of the permissible monitoring activities on an ongoing basis, it must provide an annual written notice to parents/guardians. Unlike the notice for CAT technology providers, this notice does not include a specific time of the year that it must be sent to parents. To be on the safe side, districts should be prepared to send the notice for the 2024-2025 school year by no later than the bill's effective date if it plans to engage in the permissible monitoring activities. In future years, the notice can be provided with all the other notices that are sent at the start of the school year. (See attached sample.)

B. **Requirement to Provide Seventy-Two (72) Hour Notice.** Additionally, in the event that one (1) of the permissible circumstances listed above is "triggered," a district must notify parents in writing within seventy-two (72) hours of accessing the technology. The notice must include an explanation of the circumstances which triggered the access, what features were accessed, and a description of the threat posed, if applicable. If the

notice itself would cause a threat to life or safety, districts must instead provide notice within seventy-two (72) hours after the threat has ceased. (See attached sample.)

This notice has caused a great deal of confusion and consternation for school districts. Of particular concern is how frequently the seventy-two (72) hour notice requirement is triggered. For example, some technology passively monitors data to scan for possible threats. One reading of the law might lead to a conclusion that districts must send the notice every day to parents since each student's data might be "accessed" through the technology. However, a more measured and manageable interpretation is that districts should send the seventy-two (72) hour notice whenever staff access a student's data after the technology detects a threat and links it to that student. This interpretation is supported by testimony provided by representatives when the final version of this language was proposed and later adopted.[4]

Action Steps for Part Four. Staff responsible for providing and maintaining technology in your district will need to help districts identify what access and monitoring capabilities are available on the technology, and make sure that these capabilities are turned off or strictly controlled. Administration should determine what will be monitored on an ongoing basis for the purpose of preparing the general notice, which should be drafted and sent no later than October 24th. Likewise, the seventy-two (72) hour notice should be ready for use by October 24th and sent in the event student data is accessed.

Finally, districts need to make sure that all staff, including principals and teachers, are educated so they can comply with the new restrictions and avoid unauthorized access when investigating student misconduct.

Final Reflections: What SB 29 Means for Your District

While SB 29 places some daunting requirements on districts, it isn't clear what real impact and risk schools really face from it. The bill does not indicate which enforcement agencies will be responsible for ensuring compliance with the new laws, or how they will go about enforcing them.

With so many other challenges that school districts must tackle this year, it makes sense to prioritize which tasks should be completed, and plan how they can be accomplished with the time and resources available. For instance, it is important to make sure that you follow your notice requirements if you access student data which may be used to support discipline because failure to issue a notice my subject the discipline to challenge. Likewise, this notice process is also important to document when the district accesses data related to a possible threat.

Additionally, it is perhaps more critical than ever that districts invest time in understanding their technology needs and use. Districts should have formal procedures in place to evaluate and approve new technology tools and routinely audit the technology that is currently in use. Administrators and supervisors responsible for approving and monitoring staff must become familiar with the requirements of SB 29 regarding student data privacy, technology providers, and parental notices.

Additionally, as districts renew technology provider contracts or enter into new contracts, administrators must ensure that the new provisions required by SB 29 are included in the contracts. Contracts also must still include provisions mandated by other Federal laws such as FERPA, the Children's Online Privacy Protection Act ("COPPA") which regulates operators of commercial websites and online services with regard to child safety and privacy, and the Protection of Pupil Rights Amendment ("PPRA") which governs the administration of student surveys, analysis or student evaluations that concern eight separate areas such as political affiliations, sex behavior, mental or psychological problems, etc.

It is important to ensure that contracts also include provisions related to accessibility of technology for disabled individuals, which is mandated by the Americans with Disabilities Act ("ADA"). It is advisable that districts seek legal counsel review before contracts are formally adopted to ensure terms meet the requirements of SB 29 and other laws.

[1]Districts should note that there is a small discrepancy about the official effective date of Senate Bill 29. The Legislative Service Commission and Ohio Secretary of State both recognize an effective date of October 24th. Under State law, new bills generally take effect 90 days after they are signed by the governor and filed with the Secretary of State. SB 29 was signed on July 24th, 2024, and likely filed shortly after. Some industry sources have published earlier effective dates of October 21st or October 22nd, which has caused confusion. While the discrepancy seems minor and will likely not have much impact for most of SB 29 provisions, the requirement for school districts to publish an annual notice of monitoring activities might be impacted. This is described more fully below.

[2]20 U.S.C. § 1232g, and implementing regulations codified in 34 C.F.R. Part 99.

[3]The Children's Internet Protection Act (CIPA) is a Federal law that requires schools and libraries to meet certain requirements as a condition of receiving E-Rate program discounts. Under CIPA, must adopt an Internet safety policy that includes monitoring the online activities of minors.

[4]Representative Fowler Arthur testified that "the school district or technology provider is going to generally be monitoring the school-issued device and the trigger would no longer be within seventy-two (72) hours of notice" and that "they provide the notice annually to the students' parents and seventy-two (72) hours of notice is only required when one of the specific circumstances in the bill is triggered."