Navigating Ohio SB29

Bricker Graydon

Ohio Senate Bill 29 (SB29) introduces significant changes to how schools manage, protect, and monitor student data. This guidance document is intended for school district leaders to understand these changes and how they may be practically implemented.[1]

Overview

At its core, SB29 is designed to protect the privacy of student data while ensuring transparency and accountability in how that data is monitored, accessed and used. It establishes guidelines for the management of educational records and school-issued devices, holding both schools and technology providers to a set of standards of data security. SB29 seeks to balance the need for privacy with appropriate access, ensuring that sensitive student information remains secure while still being available to those who are authorized to use it.

Key Definitions

- **Educational Records:** largely similar, though not identical to the definition of "education records" as used in FERPA. Note that certain FERPA-designated exceptions are missing, including for directory information. (R.C. 3319.325(A))

- **School-Issued Device:** 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 use. (R.C. 3319.325(C))

- **Technology Provider:** a person 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. (R.C. 3319.325(E))

Note the difference between "dedicated use" and "student use" in the definitions above. One creates a significantly broader obligation than the other. We hope that clarity on this point follows.

Contracting with Technology Providers

1. Contracts entered, or renewed, on or after October 24, 2024 MUST:

a. Ensure appropriate security safeguards for educational records, AND
b. Restrict unauthorized access to educational records, AND
c. Restrict use of educational records beyond contract fulfillment. (R.C. 3319.326(F)(1) - (2))

"Appropriate security safeguards" does not refer to a specific set of rules or regulations. For example, FERPA does not require specific security controls. Key elements of "appropriate security safeguards" may be found in publications from the National Institute of Standards and Technology (NIST). As these requirements are relatively common outside of the school district contracting space, reputable Technology providers should be willing to offer compliant terms for 1(a) - (c).

---

[1] As of this writing, we understand that the Ohio legislature is open to certain "fixes" throughout SB29, but we do not have certainty with respect to where those "fixes" may occur. As a result, our guidance here is limited to SB29 as it will go into effect on October 24, 2024, though we will highlight areas ripe for clarity.

2. Additional considerations for contracts

a. Aside from the above, R.C. 3319.326 contains a host of considerations that school districts and Technology providers should be aware of, including:
   i. Technology provider compliance with R.C. 1347, et seq,
   ii. School district ownership of educational records,
   iii. Breach notification requirements and adherence to R.C. 1347.12,
   iv. Return or destruction of educational records at the conclusion of a contract,
   v. Restrictions on how a Technology provider may sell, share, or disseminate educational records, and
   vi. Strict purpose limitations for Technology providers.

It remains unclear whether these requirements must be specifically found in contracts between school districts and Technology providers or not. School districts may face headwinds from Technology providers if the latter are required to contractually agree to R.C. 1347 ("Personal Information Systems"), as that code section contains a number of requirements that are typically only applicable to state and local agencies, including school districts.

Annual (August 1) Notification

Annually, by August 1 of each school year (starting in 2025), school districts must notify parents and students of "any **curriculum, testing, or assessment technology provider** contract affecting a student's educational records." Such notice must include:

- The identify of each such Technology provider,
- The educational records affected,
- Contract inspection information and contact information, generally.

Monitoring and Access Restrictions

1. General Prohibition:

a. School districts and technology providers cannot electronically access or monitor location-tracking features, audio or visual features, or student interactions with school-issued devices, except under specific circumstances. (R.C. 3319.327(A))

2. Specific Circumstances Where Permitted:

a. Access and monitoring is permitted provided that:
   i. The activity is limited to a noncommercial educational purpose for instruction, technical support, or exam-proctoring by school district employees, student teachers, staff contracted by a district, a vendor, or the department of education, and notice is provided in advance.
   ii. The activity is permitted under a judicial warrant.
   iii. The school district or technology provider is notified or becomes aware that the device is missing or stolen.
   iv. The activity is necessary to prevent or respond to a threat to life or safety, and the access is limited to that purpose.

i. The activity is necessary to comply with federal or state law.
ii. The activity is necessary to participate in federal or state funding programs. ((R.C. 3319.327(B)(1) - (6))

Additional Notices

1. Notice of General Monitoring

If a school district elects to generally monitor for any of the above, it must provide notice of as much to parents of enrolled students. (R.C. 3319.327(C)(1))

2. Trigger Notifications

Regardless of general monitoring, if one of the above circumstances is triggered, the school district must (absent a threat to life/safety), within 72 hours of any access, notify the student's parent and provide a written description of the triggering circumstance, including which features were accessed and a description of the threat, if any. (R.C. 3319.327(C)(2))

Note that a Notice of General Monitoring does not replace the need for 72-hour trigger notifications, when necessary. We are cognizant of the likelihood of over-notification and notification fatigue. We understand that this is an area that the legislature is paying particular attention to, as well.

Licensure

SB29 takes the long-understood prohibition on violating student confidentiality and clarifies that "using or releasing" confidential student information "for purposes other than student instruction" is grounds for the State Board of Education to refuse issuance of, limit, suspend, or revoke an educator's license. (R.C. 3319.31(B)(5))

The "for purposes other than student instruction" is likely subject to considerable interpretation, particularly as it relates to the balance of SB29's requirements.

There are likely myriad questions regarding SB29, its intent, and its practical impact on the day-to-day operations of schools, particularly with respect to IT departments. We understand that the legislature is aware of many of these questions and concerns and is open to offering "fixes" where possible. Regardless, please be prepared for SB29's effective date, October 24, 2024, and contact a member of the Bricker Graydon team with questions or concerns.