EDUCATION COMMISSION OF THE STATES
Your education policy team.

Response to information request

October 19, 2022
Zeke Perez Jr. and Claus von Zastrow
zperez@ecs.org, cvonzastrow@ecs.org

This response was prepared for the Pennsylvania House Education Committee

Your Question:

You asked for information on student data retention at the school-level, including information on types of student data retained, retention schedules, procedures for student data security and destruction, and guidance or training on student data protection and retention. Additionally, you asked specifically about the role of a state legislature in assisting these procedures and approaches.

Our Response:

State education data exists in expansive ecosystems with overlapping and differing governance structures. For instance, a state may have certain data retention requirements for school districts and may have other requirements for a longitudinal data system that shares student data across agencies. Additionally, schools and districts follow several federal and state requirements when managing student records and student data. For the purposes of this response, we focus on retention schedules for K-12 public school records.

It is important to note that many of the school-level student data retention procedures you asked about (which data are retained and for how long, how is student data secured and destroyed, and how schools protect data) are based on policy or guidance from the state or the district.

Education Commission of the States does not currently maintain a database specifically addressing record retention schedules or policies for state, district, or school student information systems. However, we can offer examples from various state agencies and data systems that house student records. Given the wide variety of education data systems within any state, our response may not be representative of all data storage, security, and retention requirements in each state example.

Types of Data Collected and Retained

The landscape of student data collection and retention is complex, with varying requirements and procedures across student information systems. A hierarchy of collection practices and governance structures exists, with school, district, and state student information systems each collecting and housing different, but overlapping, types of student data. Some state data systems publish publicly available data dictionaries that list and define the data elements that the state collects, as well as select elements collected by districts or schools for the purpose of state reporting.

In general, student information commonly collected and retained at the school level may include: personal information (name, date of birth, gender, demographic information, and social security number); student attendance data; testing data; course taking or enrollment reports; participation in extracurricular activities; and special education information. Health data, when collected, typically faces more stringent retention and destruction requirements.

In addition to student data, schools and districts also collect data on parents or guardians. Student records can include: parents' or guardians' names, contact information, and occupations; family income information (to determine eligibility for the federal school lunch program); records of permission granted for student participation

(i.e. in activities, surveys, student information requests, etc.); court records including parents' marital status or visitation rights; or notes from communications between parents and school staff.

Additionally, the education data space continues to see changes in the types of data collected and retained. With the advent of education technology, there are more types of student data collected and available than there were when many student data laws (such as FERPA) were created. These new data aren't all necessarily maintained by the school. For example, third-party education vendors (district-wide instructional supports, SEL providers, classroom apps, online gradebooks, etc.) are now collecting and storing data on student performance. This complicates the issue of data retention and destruction, prompting states to create legislation to address privacy, security, retention and destruction of student data stored by vendors.

Student Record Retention Schedules and Procedures

Typically, state statute sets parameters for record retention and designates the entity responsible for developing specific record retention schedules to be followed at various levels of data collection. Retention periods vary greatly among states (from four years to 99 years in the examples below). Even within states, retention periods vary depending on the type of data (see Michigan). This section provides state examples, as well as a district example, of student record retention policies, which may dictate how long various types of data may be retained and how they should be destroyed.

Arizona

The state's student record retention schedule was created by the Arizona State Library, Archives and Public Records and is issued to all Arizona school districts and charter schools. The schedule provides comprehensive retention periods and legal citations for an assortment of student records. A majority of student records (including disciplinary records, daily attendance records and special education records) are required to be retained for a minimum of four years, although permanent student records (including personal identifying information, transcripts of final grades and standardized test scores) and immunization records are required to be preserved permanently.

Indiana

The Indiana Archives and Records Administration issued a **retention schedule** for educational institutions. The schedule includes retention periods for individual student files such as testing result records, individualized education plans and educational placement information and individual student medical files (retained for five years beyond the provision of education or until the student reaches 21 years of age, whichever is less). The schedule also allows for parents to request earlier destruction of certain student data.

Michigan

State law (MCL **399.811** and **750.491**) requires that all public records be listed on an approved schedule identifying the minimum retention period and disposal methods for various records. All schedules are approved by the Records Management Services, the Archives of Michigan and the State Administrative Board. The record retention and disposal schedule for Michigan public schools details retention and disposition requirements for student records, including for student academic records (60 years after the student graduates), other student files (destroyed upon graduation), student testing data (five years after the student graduates) and record transfer requests (four years).

Minnesota

State law requires government entities, including school districts, to maintain various records and **requires** a retention schedule for such records. To help entities comply with these requirements, the Minnesota State Archives have developed sample **general records retention schedules**, including one for **school districts**. School districts or charter schools may adopt the sample schedule or submit their own for approval. The Minnesota Department of Education developed a **FAQ guidance document** around student record retention to help inform districts about

retention schedules and requirements. The FAQ discusses federal and state guidelines for specific types of data, including a state requirement that student cumulative records be kept permanently.

North Carolina
The North Carolina Department of Natural and Cultural Resources Division of Archives and Records is responsible for issuing the **records retention and disposition schedule** for public schools. The schedule provides requirements for academic program and curriculum records, extracurricular program records and student records, among others. State statute requires that cumulative student records, as defined in the retention schedule, be maintained permanently, including "adequate identification data including date of birth, attendance data, grading and promotion data, and such other factual information as may be deemed appropriate by the local board of education having jurisdiction over the school wherein the records is maintained." The schedule also provides retention requirements for records outside of the cumulative records and specifies conditions under which suspension or expulsion data should be expunged, including by request from a parent or guardian.

Washington
Student records are maintained according to **state statute**. The Washington State Archives through the Secretary of State provide a variety of resources related to **managing school and Education Service District (ESD) records**, including a **records retention schedule** for K-12 public schools and ESDs. The records retention schedule features a revision history (page two) noting changes to requirements over time. The schedule provides a comprehensive list of public school and student records and requirements for retention timing and for disposition actions. Specifically regarding student data, the schedule lists requirements for student learning, student administration (assignment, attendance, discipline, and student records) and student services.

Pennsylvania (Philadelphia Public Schools)
Student record retention schedules can also be found at the district-level. The district's **retention schedule** provides for disposal methods (shredding physical documents held in archives or deleting electronic files that have met their retention period). The schedule includes a retention period of 99 years for student records and provides other retention periods for records in other areas, such as school employees, facilities, or safety.

Student Data Security

Diverse types of student data are stored in various electronic and physical forms. Some systems require information to be stored on local servers or on remote servers accessed through the internet, while other information may be allowed or required to be kept in paper form. For example, **Virginia's Maintenance of Student Records policy** requires that schools have procedures for the management of all records, print and nonprint, and requires that "student education records shall be maintained in fire resistant cabinets." In addition, states' and localities' technical infrastructure has expanded to include mobile devices, which could also contain, or offer access to, student data. This growing infrastructure can complicate school security plans.

For example, the **Nebraska** Department of Education **recommends** that, in this new environment, districts develop "a comprehensive security plan" that includes physical security, network security, properly configured hardware, restrictions on who has access to different kinds of data, and staff security training, among other measures.

Additionally, some states conduct privacy audits to highlight vulnerabilities in student data storage and protection. Between 2017 and 2019, for example, the **Florida** auditor conducted **a series of audits** on school districts and postsecondary institutions to determine how well students' personal information and Social Security numbers were being protected. In 2022, the **New York** comptroller's offices **audited a school district** and found gaps in protection of sensitive information held on mobile devices owned by the district.

Training on Student Data Privacy

State leaders have noted the importance of training for effective data collection, use, and security. Without training in place, it can be difficult for district or school leaders to implement state data collection and data privacy requirements because many data users do not understand which data they should protect, why they should protect it, or how they should do so. Some states have enacted policies to provide training at the state, district, and school levels to equip employees to protect student data.

Kentucky

The state's longitudinal data system, **KYSTATS**, provides annual **training** in vital data privacy processes and protocols to all KYSTATS staff who use or review data. For example, they must secure or destroy any sensitive data that could appear in printed materials, email attachments, or files on their computers or other devices. All staff must regularly review KYSTATS' **Acceptable Use** and **Data Access and Use** policies, and they must immediately bring data security concerns to the attention of the KYSTATS executive director or information systems director.

KYSTATS' partner agencies also conduct data privacy training. The Kentucky Department of Education provides its staff regular data privacy training and integrates data privacy topics into regular agency events throughout the year, including monthly webcasts or student information system meetings. The agency's website features **training resources** for schools and districts. The statewide student information system promotes similar training across district and school staff, because the state and all its 171 school districts use the same system for collecting student information.

Utah

The state's 2017 data privacy law requires local school boards to provide training and mandates training for anyone authorized to access education records. To enforce training requirements, the law requires each public school to maintain a list of individuals with access to data and requires each school board certify that each of those individuals have completed training.

Additionally, the state board of education **Administrative Rule R277-487-14** makes data privacy training a mandatory component of teacher re-licensure. To support that requirement, the state superintendent is directed to develop student data security training for educators. Teachers who are renewing their educator licenses must now complete the state's interactive online Utah Student Data Privacy Educator Course.

Wisconsin

The department of public instruction offers an online **suite** of training materials that cover topics like protecting student data, sharing information across systems, managing different kinds of student records and complying with federal law. The materials include videos and **an online course** users can complete at their own pace.

Legislative Approaches

State legislation and other state policies play a vital role in establishing requirements for, and enforcing, data protection, retention, and safety in schools. The following examples are far from exhaustive, but they demonstrate efforts legislatures may take related to promoting student data privacy in districts and schools.

Maryland **H.B. 245** (Enacted 2019)

This bill created a Student Data Privacy Council to review the implementation of the state's Student Data Privacy Act of 2015, study other states' laws, consider the impact of technology developments, and recommend any appropriate statutory or regulatory changes to the governor and General Assembly. In its **January 2021 report**, the council recommended strengthening enforcement of data privacy requirements and improving transparency around privacy. In 2022, the legislature adopted several recommendations in **H.B. 769**.

Utah H.B. 358 (Enacted 2016)
This bill created a state data governance structure and appointed a student data officer to promote a more coherent data privacy infrastructure across the state. It also requires each district to form its own data governance policies and designate a student data privacy manager to build local capacity for data protection. In addition, it established an advisory group of district and school data users who offer input into the feasibility of proposed data policies.

West Virginia H.B. 4316 (Enacted 2014)
This bill outlines state responsibilities for maintaining and publishing an inventory "and dictionary or index of data elements with definitions of individual student data fields in the student data system." In addition, the bill prohibits schools and districts from providing the state with individual student data on such topics as juvenile delinquency records, criminal records, medical records, biometric information, political or religious beliefs, or sexual orientation.

Additional Resources and Organizations

Education Commission of the States, 50-State Comparison on Statewide Longitudinal Data Systems
This database looks at state data systems that connect student data across at least two of four core agencies: early learning, K-12, postsecondary, and workforce. It features information on states that publish **formal data privacy policies** for their longitudinal data systems.

Data Quality Campaign
DQC offers a wealth of information on data collection and use, as well as resources on **prioritizing privacy** in data efforts.

Future of Privacy Forum
This **organization** provides resources for a variety of audiences on education data privacy, including a resource page on **Youth & Education Privacy**.

Student Privacy Compass
This **online resource** "aims to provide a one-stop shop for education privacy-related resources to all stakeholders in the student privacy conversation: students, parents, educators and education agencies, the edtech industry, and policymakers struggling to grapple with the ever-changing student privacy legal landscape." It includes a **database of state student privacy laws** that is sortable by sector (early education, K-12, higher education) and entity subject to regulation (vendors, state education agencies or local education agencies.)