

Data Retention Study of Local Education Agencies | 2026

Utah State Board of Education

Report to the Utah State Legislature Education
Interim Committee



Utah State Board of Education

Trish Joshua
Senior Research Analyst
Trish.Joshua@schools.utah.gov

Table of Contents

Table of Contents	1
Executive Summary.....	3
Key Findings	3
Recommendations	3
Introduction	4
The Data System and Reporting Advisory Committee	4
Methodology	4
Study Relevance	6
Changes in Modern Data Collection	6
Data Privacy, Cybersecurity, and Recent Incidents.....	6
Relevant Legislation	7
Background on Data Retention in Utah	7
Definitions	7
LEA Responsibilities.....	8
Utah Division of Archives and Records Service (DARS) Retention Support.....	9
Utah State Board of Education Retention Support.....	10
Current USBE-DARS Involvement in Retention	10
Student Data Collection.....	11
Definition of Personally Identifiable Student Data	12
Study Findings about Student Data Collection.....	12
Legislative Requirements	13
Storing Student Data.....	14
Systematic and Incidental Data Storage.....	14
Version Control.....	14
On-Premises and Cloud-Based Storage	15
Infrastructure Data.....	15
Understanding Data Retention	15
Tracking Data Retention.....	17
Student Information Systems	17
Google and Microsoft Productivity Suites.....	18
Physical Paper Records.....	20
LEA-Issued Staff Devices.....	22
Third Party Applications	23
Securing Data.....	24
Student Information Systems.....	24
Google and Microsoft Productivity Suites.....	24

Physical Paper Records.....	26
LEA-Issued Staff Devices.....	26
Third Party Applications	27
Catalysts for LEA Data Retention	28
Data Retention for Special Education Records.....	28
Storage Constraints.....	28
Obstacles to Data Retention.....	30
Data Needs.....	30
Lack of Awareness and Clarity.....	33
Competing Priorities for Resources	36
Technological Constraints	38
Too New to Worry About Data Retention	39
Unclear Responsibilities within an LEA.....	40
Recommendations	40
Implementation Considerations.....	42
Appendix.....	45
Appendix A: The Data Systems and Reporting Advisory Committee	45
Appendix B: Interview Questions	47
Appendix C: Compliance with Cybersecurity and Data Privacy	48
Appendix D: Personally Identifiable Student Data.....	49
Appendix E: Necessary Student Data	50
Citations.....	52

Data Retention Study

Executive Summary

Utah Code [§ 53E-3-526](#) required that the Utah State Board of Education (USBE) examine the student data retention practices among Local Education Agencies (LEAs) in Utah and compile a report.

Key Findings	Recommendations
• Inconsistent Compliance • Unclear Ownership • Barriers to Retention	• Modernize • Support • Clarify

Key Findings

- Most LEAs are not following record retention schedules for most of their records.
- There is no clear ownership between LEAs, USBE, and Utah Division of Archives and Records Service (DARS) over LEA data retention technical assistance support and the responsibility to request an update to outdated or missing general retention schedules, leading to a lack of clear guidance and standardization of record retention schedules.
- LEAs cited obstacles to data retention, including a desire to keep data past retention schedule limits, a lack of awareness and guidance, low prioritization, and technological constraints.

Recommendations

1. One new set of education retention schedules should be created and adopted by all LEAs.

2. The new set of education retention schedules should be accompanied by education-specific resources and training for all LEA staff including Appointed Records Officers (AROs).
3. The USBE, the Legislature and DARS should clearly delineate ownership and responsibilities for creating, maintaining, and providing guidance on the new set of education retention schedules.

Introduction

Utah Code [§ 53E-3-526](#) required that the Utah State Board of Education (USBE) examine student data retention in local education agencies (LEAs) and present a study. To determine methods used by LEAs to store data and manage data retention, interviews were conducted with a variety of staff in multiple LEAs throughout Utah.

The Data System and Reporting Advisory Committee

In accordance with Utah Code [§ 53E-3-526](#) and under the guidance of USBE Board leadership, the Data Systems and Reporting Advisory Committee was formed with a variety of required stakeholders. Members were selected based on their relevant experience and to ensure varied representation. The committee was finalized at the end of May 2025 and met regularly until September 2026.

This committee advised on the study, methodology, and voted on final recommendations. They provided critical insight into LEA experiences. See [Appendix A](#) for more information.

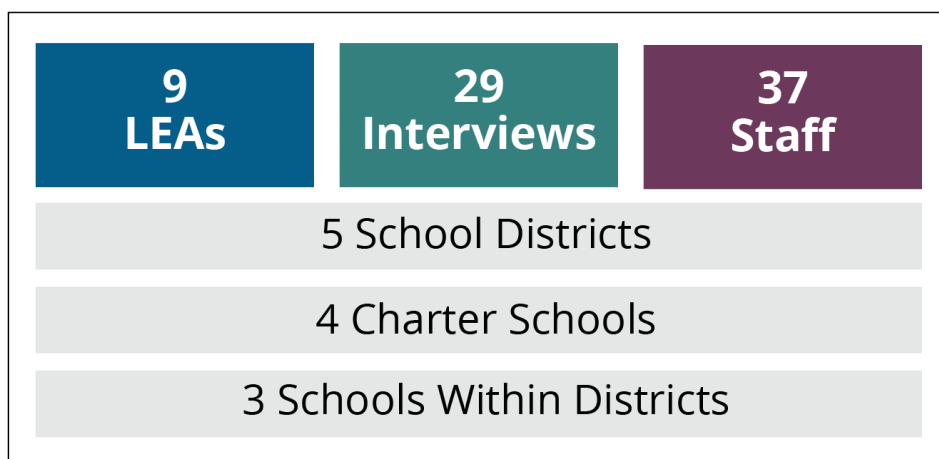
Methodology

LEA Interviews

29 in-depth data retention interviews were conducted with 37 staff from nine LEAs.

LEA Selection

To fulfil the requirements of the law and gather the needed LEA insight, two USBE staff visited a variety of LEAs. LEAs were chosen to prioritize a variety of Utah regions, LEA types, and sizes. Two large school districts, one medium school district, and two small, rural school districts were interviewed. Three schools were also visited within school districts: one elementary school and one high school from two rural districts as well as one high school from a large school district. Four charter schools were interviewed: one online-only charter school, one small charter school, and two large charter networks.



Staff Selection

A range of staff members were interviewed at each LEA. In total, 37 staff members were interviewed.

LEAs have unique job titles and often one person fills multiple roles in an LEA. In the list below, general job titles have been used to preserve anonymity of interviewees.

Roles of LEA Staff Interviewed

- Attendance Secretary
- Business Administrator
- Career and Technical Education Director
- Certified Records Officer
- Charter School Executive Director
- Cybersecurity Specialist
- Data Manager
- Digital Teaching and Learning Specialist
- District Superintendent
- Financial Secretary
- Front Desk Secretary
- IT Administrator
- IT Director
- McKinney-Vento Specialist
- Medicaid Specialist
- Office Administrator
- Paralegal
- Programmer
- School Counselor
- School Nurse
- School Psychologist
- Special Education Director
- Special Education Secretary
- Special Education Teacher
- Student Information System Manager
- Transportation Director

Interview Questions

Interview questions, available in [Appendix B](#), were based on the study requirements outlined in Utah Code [§ 53E-3-526](#). Questions were standardized for all LEAs interviewed.

Compliance with Cybersecurity and Data Privacy

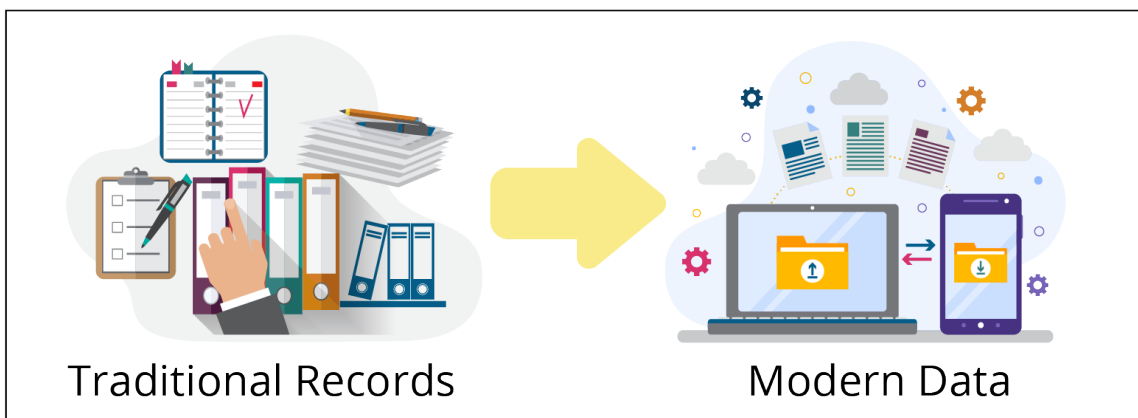
Utah Code [§ 53E-3-526](#) included a requirement to examine LEA compliance with privacy requirements in legislation and cybersecurity standards in USBE administrative rule. This information is included in [Appendix C](#).

Study Relevance

Changes in Modern Data Collection

In recent decades, many education agencies have shifted priorities toward an emphasis on data-driven decision making. In a sprint towards easily accessible and detailed data, LEA are adapting, reconsidering, and modernizing their previous physical documentation processes. In the midst of these changes, decades old data

retention best practices focusing on physical paper records have quickly gone out of date.



However, both the increase in the quantity of data and the consolidation of data pose threats to data security and data privacy.

Data Privacy, Cybersecurity, and Recent Incidents

According to the U.S. Government Accountability Office, cyber incidents in public education have grown from 400 in 2018 to 1,300 in 2021, the most recent available data (U.S. Government Accountability Office, 2022).

One notable, recent cyber incident at a Utah school district impacted the personal data of 450,000 students and 30,000 employees. In addition to overtime staff costs to respond to this attack, this school district paid \$150,000 to their cyber insurance provider (Office of the Legislative Auditor General, 2025).

Beyond attacks that targeted LEAs directly, many education technology companies have experienced cyber incidents. Most notably, in the past two years, two commonly-used education technology companies—a student information system (SIS) and a learning management system—experienced cybersecurity incidents that reportedly impacted many current and former students, families, and staff.

An increase in national incidents and incidents in Utah bring cybersecurity and privacy concerns to the foreground for many stakeholders and highlight the

importance of minimizing the data collected and retained by LEAs and their partners.

Relevant Legislation

The following pieces of Utah legislation and USBE administrative rule inform LEA data retention.

- [Utah Code § 63A-19](#): Government Data Privacy Act (GDPA)
- [Utah Code § 63G-2](#): Government Records Access and Management Act (GRAMA)
- [Utah Code § 53E-9](#): Utah Student Privacy and Data Protection Act
- [Administrative Rule R277-487-4](#): Public School Data Confidentiality and Disclosure

Each of the above laws describe an LEA's obligation to maintain and destroy student records.

Background on Data Retention in Utah

Definitions

Retention Schedule

A **retention schedule** identifies how long a government agency is required to keep a record in a record series and what to do with the record when it is no longer needed.

Disposition

Disposition is the final state of the record: either maintained permanently or destroyed.

LEA Responsibilities

LEAs are responsible for following record retention schedules just like all other government agencies. An LEA must have retention schedules adopted for all records. This can be done by individual schools within a school district, by districts or by charter schools.

LEAs can look through general retention schedules (GRS) on the Utah Division of Archives and Records Service (DARS) website. Through this website, they may be able to find a GRS that closely aligns or matches their records that they must adopt unless they choose to create their own agency-specific retention schedule.

If an updated or new retention schedule is needed, LEAs are responsible for this process. This is true even when legislation passes that requires all LEAs to change their retention schedules or add a new record.

When a record retention schedule must be updated or created, LEAs must complete one of the following two options.

1. LEAs can go to DARS to file with the Records Management Committee for the establishment of a new or updated GRS. The Records Management Committee reviews and approves retention schedules. Even when a change

would affect all LEAs, an LEA would need to initiate this process in order to change or add a GRS.

2. LEAs can create and maintain their own agency-specific retention schedules because they are governmental entities. However, before adopting an agency-specific retention schedule, DARS must review the schedule to ensure that historical records are being preserved. If LEAs decide to maintain their own retention schedules, those retention schedules cannot be adopted by any other agencies, including any other LEA.

These processes are time consuming and involve justifying schedules with the DARS Records Management Committee.

Utah Division of Archives and Records Service (DARS) Retention Support

The Utah Division of Archives and Records Service (DARS) assists government agencies in managing records and providing access to public information.

With about 30 staff members, DARS provides support to all governmental agencies like USBE, the Utah tax commission, the Utah Department of Agriculture and Food, the Utah Supreme Court, higher education entities, cities and towns, and more. One DARS employee is responsible for supporting all LEAs, USBE, all higher education entities, as well as other state agencies. Support for LEAs can include providing on-site training, consultation calls, and creating agency-specific schedules for LEAs as requested. DARS also maintains an online searchable catalog of GRSs as well as available agency-specific schedules.

DARS establishes GRSs and agency-specific schedules at the request of an LEA, only once the LEA has identified a record and proposed a retention schedule. DARS does not proactively create retention schedules on behalf of LEAs.

Despite available resources, a DARS employee reported that less than 25% of LEAs are in communication with DARS annually. There are a variety of reasons for this, which are discussed further in [Obstacles to Data Retention](#).

Appointed Records Officers

LEAs are required to have an Appointed Records Officer (ARO) who must successfully complete online training and obtain certification annually. AROs can be appointed at the school level or district level, depending on the LEA. DARS provides this certification as well as training on the Government Records Access and Management Act (GRAMA) and Records and Information Management (RIM). The DARS website hosts additional resources, including a record and information management webinar series. These resources are general to government agencies and do not include any specific training for LEAs.

Records Center and Archives

DARS provides a Records Center, where paper records that have not met their retention schedule can be stored free of cost to LEAs. These records have not reached their final disposition of permanent retention or destruction.

Separately, DARS maintains archives, which permanently preserve records of historical value in any format. DARS is currently not collecting digital records, as they are in the process of obtaining a Digital Asset Management system to preserve digital records more efficiently.

Utah State Board of Education Retention Support

USBE has no dedicated staff for data retention support. Historically, however, a member of the Student Data Privacy team at USBE has fielded questions and shared resources about data retention. The USBE does not update or add new retention schedules for LEAs.

Utah Records Appraisal and Management Program (RAMP)

In response to LEA requests for assistance, USBE released the [Utah Records Appraisal and Management Program \(RAMP\)](#) in 2020. The RAMP provides LEAs with a set of retention schedules created to serve as a guide for LEAs. At the time, DARS and the USBE recommended LEAs adopt the Utah RAMP. In addition to the RAMP, a quick guide resource summarizing parts of the RAMP was released. These resources are no longer being updated.

Current USBE-DARS Involvement in Retention

While data minimization is key for data privacy and security and could be considered relevant to the work of USBE's data privacy team, USBE does not have a legislative obligation to ensure LEA compliance with data retention schedules. This has led to questions about whether it is appropriate for USBE staff to devote the time needed to support LEAs with record retention. Additionally, USBE does not have the records expertise of the DARS staff. However, relying on DARS to conduct all support for LEAs regarding data management presents issues because some questions require a high expertise and background knowledge in public education. This gap is illustrated by the example below.

Case Study: Seclusion Room Camera Footage Retention

In the 2026 legislative session, LEAs were mandated to collect a new record, an audio and visual recording of an LEA's designated seclusion room. Utah Code [§ 53G-8-301](#) requires LEAs to follow "retention requirements established by the state board in rule...", thus USBE has attempted to provide LEAs with a new retention schedule for this new record.

DARS staff have supported the USBE staff member in determining the need for a new general retention schedule; however, the specifics about what that schedule should be were left up to the USBE staff. This staff member then spent weeks speaking to subject matter experts at the USBE and in the LEAs. Finally they presented their retention schedule to the DARS, who must now approve and establish the GRS.

If not for the mention of USBE, an LEA would have needed to request a specific new GRS and go through this time-intensive process or else there would not be a directly applicable GRS for this new record.

Student Data Collection

To fulfill the requirements of Utah Code [§ 53E-3-526](#), the following section gives an overview of some of the student data that is collected by LEAs. It is complicated to attempt to create a complete list of all student data collected, as each LEA is distinct and includes a variety of staff that may collect different pieces of student data.

Further complicating, LEAs collect pieces of student data for a variety of purposes in a variety of formats.

Definition of Personally Identifiable Student Data

LEAs collect many distinct pieces of personally identifiable student data. According to Utah Code [§ 53E-9-301\(15\)\(a\)](#) "Personally identifiable student data" means "student data that identifies or is used by the holder to identify a student." Utah Code [§ 53E-9-301\(15\)\(b\)](#) identifies examples of personally identifiable student data, the full list included can be found in [Appendix D](#). These include traditional identifiers, such as a student's name and birthdate. However, it also includes indirect identifiers, including "information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty."

Study Findings about Student Data Collection

The following are types of student personally identifiable information that were identified by the 37 LEA staff interviewed. This is not a comprehensive list of student data collected by LEAs and is intended to provide general insight.

List as Shared by LEA Staff Interviewed

- Academic Records
- Athletics data
- Attendance
- Behavioral Records
- Bus Ridership Data
- Contact Information
- Class Schedules
- English Language Learner Status
- Family Custody Information
- Fieldtrip data
- Financial Records
- Health Records
- Identification Documents
- Immigration Documents
- Individualized Education Plans
- Internet activity/device usage
- Juvenile Criminal Information
- McKinney Vento Status
- Proof of Residency Documents
- Recommendation Letters
- Security Camera Footage
- Student and Teacher Microsoft and Office Productivity Suite Content
- Student Demographics
- Student ID Numbers
- Testing Information
- Transcripts

Many LEA staff explicitly shared that they did not collect social security numbers and biometric data.

Legislative Requirements

Many pieces of student data are collected because of legislative requirements. Some can clearly be tied to a single or a few pieces of legislation.

- For example, Utah Code [§ 53G-6-604](#) was amended in 2026 to require that when a student transfers schools, the student record includes “the student’s discipline file including any safe-school violation, reintegration, or threat assessment.”

Some types of student data, however, cannot clearly be linked to legislation but are practically ubiquitous in legislation about data collection; for example, a student ID number or student name.

There are a few resources below that can provide further insight into some of the student data LEAs collect.

UTREx Specifications Manual

The [UTREx Specifications Manual](#) guides LEAs in the submission of data through their SIS to USBE. This list can offer insight into what LEAs collect because they are required to submit the data to USBE.

USBE Reporting Requirements Study

The USBE Reporting Requirements Study mandated by Utah Code [§ 53E-3-526](#) includes a catalog of reporting requirements and a description of required data elements. This list can offer insight into what LEAs collect because of requirements to submit the data to USBE, the state and federal government.

Utah Code Defining “Necessary Student Data”

Utah Code [§ 53E-9-301\(12\)](#), defines “necessary student data” as “data required by state statute or federal law to conduct the regular activities of an education entity”. This definition outlines a number of pieces of necessary student data, the full list can be found in [Appendix E](#).

Storing Student Data

There are a few primary locations where most LEA data is created or gathered: student information systems, Microsoft and Google productivity suites, physical paper records, LEA-issued personal staff devices, LEA-maintained servers and backups, and third party applications. Each storage location presents unique challenges to data retention, as described in the [Tracking Data Retention](#) section of this report.

Systematic and Incidental Data Storage

Some storage is gathered and purposefully stored systematically in an SIS, local servers, or shared with a third party. Other student data storage can be incidental, such as when a teacher creates a note about a student in their LEA-issued device. This type of data storage is common in LEAs, as staff create seating charts, email parents, make behavior logs, birthday calendars, newsletters, and more.

Systematic	Incidental
• SIS • Servers • Third-Party Systems	• Teacher Notes • Email • Seating Charts • Behavior Logs • Calendars • Newsletters

Version Control

In addition to systematic and incidental data storage, staff often make copies or download records, making another version of these records. According to DARS best practices, when an official record copy—the definitive document that is retained for the full retention schedule—is destroyed, all of the other duplicates or versions must also be destroyed. They can be destroyed before the record copy, but must not be retained after the record copy has been destroyed.

This poses significant issues for LEAs. Those at an LEA responsible for data retention do not have access to determine if duplicates were made or downloaded and where they might be stored.

On-Premises and Cloud-Based Storage

Data storage is complex. Modern data storage includes storage on local servers on-premises as well as cloud-based storage. When data is stored on-premises at an LEA, staff have more control over the maintenance or security of the data.

Increasingly, however, critical infrastructure applications like Google, Microsoft, or commercially available student information systems have complex cloud-based storage. Cloud-based storage means data is saved on remote servers and then accessed through the internet.

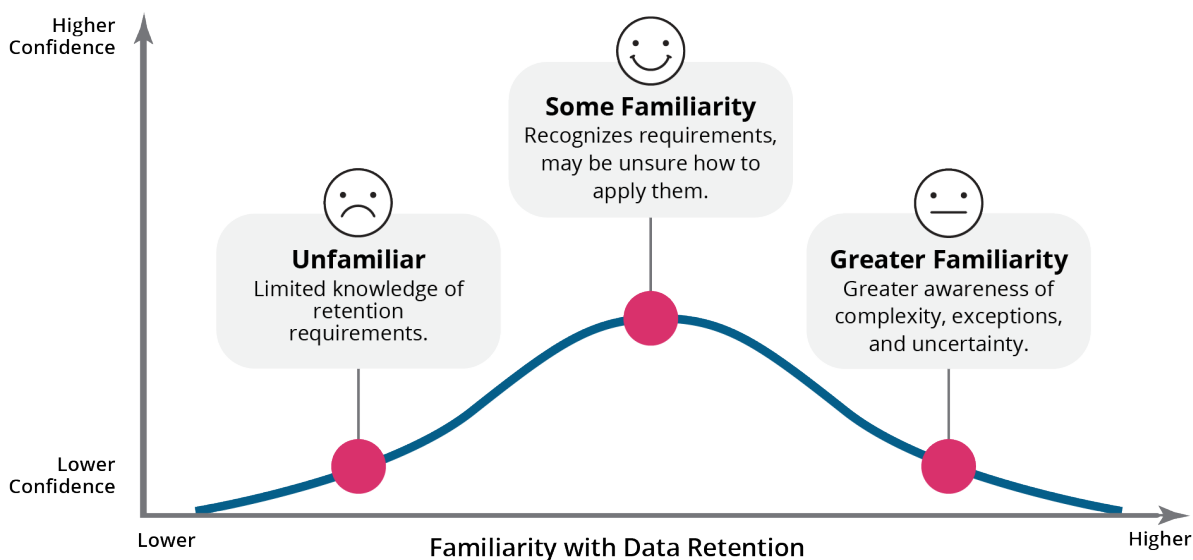
Cloud-based storage systems make it increasingly difficult to answer questions about where data is physically stored as data may be stored in a number of different data centers in many different places. LEA staff may also have little control or awareness over how often cloud-based storage systems create backups and how often these backups are being erased. It could be that a document is deleted, but the backup of that document is retained.

Infrastructure Data

In addition to other storage locations, some IT services, like active directories used for computer account management, are necessary for operations but also require student data storage.

Understanding Data Retention

There was a broad range of levels of familiarity and confidence among LEA staff interviewed about data retention. Generally the staff most confident about data



More familiarity did not always mean more confidence.
Greater understanding sometimes revealed just how complex data retention can be.

retention were those at a basic level of familiarity with some aspects of data retention schedules. The more staff learned about the intricacies and applications of data retention, the less confident they felt. This is notably illustrated by the case study below.

“I have a good sense of the RAMP document, but it’s harder to implement than what meets the eye.”

- District SIS Manager

Familiar and Confident

Despite their high confidence, some LEA staff had inaccurate information about retention. In one case, an LEA staff member mentioned they were extremely confident and familiar, while later disclosing that their policy was to retain all student data, highlighting the disconnect between perceived and actual knowledge.

Some staff felt confident because of resources provided to them. An office manager in a high school, and a business administrator in a charter school, felt confident as they pointed to quick guides based on the RAMP created, but not updated by USBE.

Familiar, but Not Confident

Some staff were familiar with data retention, but did not feel confident in their application of data retention practices.

Two of these staff members were SIS data managers in two districts. One primarily used the RAMP to find information about data retention and the other primarily tried to use the DARS website directly. Neither felt equipped to properly tackle data retention in their district.

Unfamiliar

Many staff members were unfamiliar with data retention. In one case a staff member was not familiar with the term, “data retention”, but had a retention plan that they adhered to strictly for one record. A staff member who worked supporting students under the McKinney-Vento Homeless Assistance Act as well as a school nurse responsible for many student health care plans had never heard of data

retention practices at all. The school nurse asked many times throughout the interview if they were doing the right thing and if the interviewers would return to give guidance.

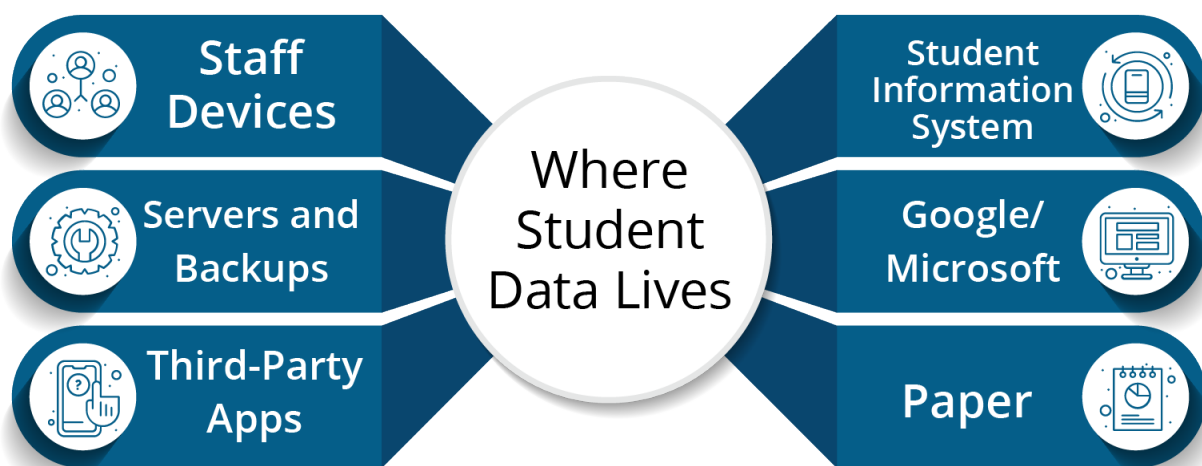
Case Study: ARO and School Secretary

In one LEA, an ARO created a retention guide specifically for their district. The ARO shared in their interview that they did not feel confident in their data retention practices. They mentioned many questions about records retention and inconsistencies with the GRS.

Later, when interviewing a school secretary in that same ARO's school district, the school secretary reported strong confidence in their retention practices. Those practices were primarily rooted in the guide created by the district ARO.

Tracking Data Retention

In general, LEA staff interviewed struggled to confidently comply with data retention requirements. Different data storage locations offer some unique challenges to data retention.



Student Information Systems (SIS)

All LEAs maintain systems for collecting and storing student data that are then submitted to the USBE. These systems are called SISs. They primarily manage and

store data but also serve as a central platform for grades, scheduling, enrollment, attendance, and more. Typically most staff at an LEA have some access to their LEA's SIS. There are currently eight different SIS being used by LEAs in Utah. These include a USBE-provided system (Aspire), two home-grown systems (Davis and Sevier), and five commercially available systems.

SIS data is often stored in some kind of back-end data warehouse or data lake. These can be cloud-based or stored on LEA local servers. These data warehouses are often purchased software solutions for organizing complex data, while SISs typically focus more on day-to-day operations.

SIS Data Retention

Only one of the LEAs interviewed mentioned that they routinely delete information from their SIS. All other LEA data managers or SIS managers reported that their policy was to keep all data indefinitely.

**Only one of the LEAs interviewed
mentioned that they routinely delete
information from their SIS.**

Most staff have the ability to update or add information, but only IT in many schools could delete data stored in the SIS. One charter school office manager mentioned that if data needs to be deleted, they have to reach out to their network charter office administrator.

Google and Microsoft Productivity Suites

Most LEAs use productivity suites like Google Workspace or Microsoft 365 that offer a wide variety of services such as email, cloud storage, document creation, collaboration, and more. These productivity suites store student and staff emails, photos, chats, documents, presentations, spreadsheets, surveys, and in some cases, AI chat histories. These suites also house staff-generated and student-generated content, much of which can have systematic and incidental storage of personally identifiable student data.

The kinds of data stored in these systems was very diverse: a teacher uses these systems to collaborate on lesson plans, a registrar manages schedules and enrollment, a school secretary tracks field trip information and attendance, a school psychologist keeps health and behavior logs, and teachers at an online school store class recordings.

"It is scary to imagine what is stored on the Google Drive... I hope people aren't taking data out of our systems and storing it on their Google Drive, but I am sure they are. I am not sure how much we can control that...."

- SIS Data Manager

Google and Microsoft Productivity Suites Data Retention

Retention schedules for Google and Microsoft productivity suites are complex because there is a student or staff account, which could be deleted, but there are also many records within the account which have their own distinct records schedules.

There was no standard approach to data retention in productivity suites for LEAs. The following examples for district policies on general staff and student accounts highlights the broad range of LEA practices.

LEA Policy for Retaining Staff Accounts

- One large charter network has a policy to keep everything that teachers have on their Google drives. In fact, in the past when a teacher has deleted records during offboarding, IT has restored the data.
- One small rural district shared that they cannot dispose of employee accounts. This staff member said that they had been given guidance to retain this data forever.
- One large school district deletes chats, but stores all emails indefinitely.
- One large school district retains staff accounts with all data, including Gemini chats, for seven years.

LEA Policy for Retaining Student Accounts

- One small rural school district keeps student accounts for four to five years.
- One large school district keeps student accounts indefinitely.
- One large charter school network is considering starting to delete Google drive accounts 10 years after their last login. However, they have not yet begun this process.

LEA Policy for Specific Records within Google and Microsoft Productivity Suites

Besides general LEA policies around retention of student or staff accounts, particular records within productivity suites have separate retention schedules that must be accounted for. No LEA interviewed had clear guidelines around all records in Google or Microsoft Productivity Suite. Some LEA staff had retention schedules for some records that they personally maintained, but no LEA staff knew of guidelines for records in productivity suite accounts that were not theirs.

The following are a few examples of staff with retention schedules for specific records on their Google and Microsoft productivity suites.

- One online charter school had strict retention schedules around Google folders. They maintain all student data online and have a folder of data for

each student. As soon as a student separates from the school, they put a timestamp on the name of all student files to track data retention.

- An administrative secretary had a strict retention schedule for a certain type of document kept in the Google drive.
- A medicaid specialist and special education records secretary also had clear processes surrounding special education records kept in their Microsoft and Google productivity suites.

Despite these cases, the vast majority of staff had no retention practices for their productivity suites. This includes a career and technical education director, an SIS manager, an office secretary, a school counselor, a school nurse, a school psychologist, and a charter school director.

Physical Paper Records

Many LEAs are moving away from physical records. Staff interviewed, particularly leadership at the district or administrator level, frequently did not personally create or store any physical papers with student personally identifiable information.

Despite this, LEAs continue to manage a variety of physical paper records. These records include transcripts, copies of student birth certificates, special education files, fee waivers, attendance, immunization records, registration information, student custody information, club enrollment, permission slips, and more.

These physical records are stored in faculty rooms, storage closets, basements, front desks, and staff offices, among many other locations.

Physical Paper Records Data Retention

Overall, physical papers represents the most widespread use of retention schedule as well as record destruction or archiving in LEAs.

Physical Paper Record Destruction

All but one of the staff interviewed that manage physical papers destroyed those records. Typically, these were destroyed by shredding, either using a paper shredding company or an LEA shredder.

LEAs had different norms around paper destruction.

- One high school taped up boxes filled with their documents and labelled them with the year to be destroyed each summer.
- At another LEA, special education staff work together for one day a year to store files and destroy the oldest records.

Physical Paper Records to Archives

While physical paper records are most likely to be sent to archives of all record formats, LEAs are infrequently sending paper records to DARS to be archived. This is contrary to many retention schedules; for example, according to retention schedules, transcripts must be submitted to DARS after 40 years. This schedule means that every LEA over 40 years old should submit yearly transcripts to the DARS archives. However a DARS staff member estimated that less than 10 LEAs send records to archives each year, suggesting underutilization and non-compliance.

- Only one large school district reported regularly sending physical papers to DARS.
- Only two of the interviewed LEAs had ever sent physical papers to DARS for archiving.

LEA-Issued Staff Devices

LEAs issue computers to staff and most offer computers to students. Some LEAs also offer other devices like tablets. These devices allow storage on their local hard drives.

Examples of student data that interviewees store on their devices include an entire SIS backup, school bus camera footage, transcripts, health records, and student- or staff-generated content. LEA-issued devices also typically store anything that the staff or student has downloaded.

LEA-Issued Staff Devices Data Retention

No LEA staff member interviewed discussed any formal processes for tracking data retention on LEA-issued devices' hard drives. Many staff mentioned personal habits of deleting downloaded data and most were motivated to do so because of a lack of storage space on LEA-issued computer hard drives.

An example of the range of practices for staff deleting their device downloads includes one LEA deleting immediately, another once a week, another every month, and another every three months.

Reimaging or Retiring Devices

LEAs interviewed often had procedures and systems for wiping or reimaging staff devices when a device needs to be updated or a staff member separated from the school. The length of time that LEA-issued devices are rotated depends on the LEA.

- One large school district rotated devices at schools every three to four years for students and four to five years for employees.

Once a device is rotated, data stored on the computer hard drives is wiped, which should mean that the data that was maintained there is destroyed. However, some LEA IT managers shared that often the process of reimaging devices includes copying all data from one hard drive to another or onto a Google or Microsoft productivity suite. Potentially, these practices could lead a staff member to be able to retain student information for an entire 25 year career across multiple devices.

Third Party Applications

Third party applications are used in LEAs to create, track, and maintain school fees, curriculum materials, lunch management, behavior data, special education records, school transportation routes, grades, family communication, and more. Other third party applications are used for instructional purposes, such as learning management systems and curriculum software. In order to facilitate these varied purposes a variety of data is shared and stored in the third party applications.

Utah Code [§ 53E-9-309](#) requires provisions related to privacy to be included in a contract when data is shared with a third party, including provisions related to data retention and destruction. The law does not specify a particular kind of contract that must be used to meet this requirement, but the most common method is through the use of the National Data Privacy Agreement (NDPA), provided by the Student Data Privacy Consortium.

Third Party Data Retention

One of the terms of the NDPA is a requirement that data shared from the LEA to the third party is destroyed after termination of the contract, or upon request of the LEA. LEA data managers are trained by USBE to request data destruction and a certificate of destruction from third parties.

- Four data managers interviewed reported requesting data destruction from a third party application, while two assumed that the third party would delete the data when the contract was terminated without follow up.

Some LEA data managers reported receiving pushback from third parties when requesting data destruction, with some companies that desire to maintain student data past a contract.

Securing Data

LEAs use different methods to secure stored data, depending on the format the data is stored in. The following are some descriptions of the types of security methods taken by LEAs for each format.

Student Information Systems

Access Controls

Most SISs have access controls that can assign users permissions to view certain elements of data while limiting access to other information.

Password Protection/Multifactor Authentication (MFA)

Most LEA staff interviewed mentioned that their SIS was password protected. A medium sized school district and large school district mentioned that their SIS required multifactor authentication (MFA), which is a requirement to use two or more verification factors to authenticate your identity before gaining access.

Physical On-Premises Servers

LEAs interviewed who store their SIS in on-premises data centers also reported robust physical security, including around the clock monitoring, alarms, and limited access to entry.

Google and Microsoft Productivity Suites

“We are constantly getting scam emails.”

- LEA Business Administrator

Password Protection and MFA

Many staff mentioned password protection and MFA to access their Google and Microsoft productivity suites.

- One large school district requires complex passwords to be changed every 6 months.
- When one LEA first began incorporating MFA, a few years ago, there was outrage and frustration among their staff, particularly from veteran teachers. Now, however, this is a commonplace practice at the LEA and most teachers use their personal devices to authenticate.

Share Controls and Email Restrictions

Google and Microsoft productivity suite accounts, for both staff and students, offer a number of possible controls that can be implemented for sharing documents and other files. Additionally, productivity suites offer controls to allow or limit the sending and receiving of emails.

Generally, many LEA staff expressed their caution with sharing data from their productivity suites, either through sharing files or by sending emails. Many explained their best practices of double-checking and confirming recipients as well as ensuring that the recipient was receiving only the necessary level of accessibility. Other staff warned against sending files on Google that are “viewable by everyone with a link”.

Teacher Emails/Sharing

- In two charter school networks and one large school district, staff can share files outside the organization, but are asked to refrain by LEA leadership.

- In one large charter school network and a large school district, staff are alerted before sharing a file with someone outside of their organization.

Student Emails/Sharing

- In two charter school networks, students can only receive emails from teachers and can only share files with those within LEA staff.
- In one school district, students can email outside of the LEA, but can only begin to share files with someone outside of the organization during their senior year of high school.
- In one small rural district, students can only share files with their teachers.

Training

One small rural school district, one large school district, and two charter schools have some LEA teacher training related to access controls on their productivity suites. In one LEA, sharing precautions are addressed as a part of beginning of year staff training.

Physical Paper Records

The primary method LEAs mentioned for securing physical paper records was physical security with locks, badges and keys. Some LEAs also mentioned sign in or front desk security.

Locks

Filing cabinets, drawers, and offices with documents were locked in large and small charter schools and school districts. These LEA staff also often mentioned that there was limited access to the keys or badges.

LEA-Issued Staff Devices

Most LEAs interviewed manage their own technology given to staff, but one small charter school works with a company to manage IT.

Computer Screen Timeout/Logging Out

- Staff members from a small, medium, and large LEA mentioned consistently logging out of their computer when they were away.

- A small charter school and a large school district staff member shared that they implement a computer screen timeout for staff computers.

Password Protection

All staff interviewed shared that their computers require sign in with password protection.

- One staff member with access to medical records shared that they use the same password for all of their accounts, including their LEA-issued devices.

MFA

Staff members from two small districts, one medium district, one large district, and one large charter school mentioned using MFA for staff logging into their LEA-issued staff devices.

There are few realistic possibilities for MFA for student accounts due to concerns with students using their own personal devices for authentication, processing biometric data, or supplying fobs for all students.

Encryption

One school mentioned that their computers are encrypted, which requires the use of a password to access all data on the hard drive.

Third Party Applications

There are many types of third party applications. Security controls vary by application; some protections include password protection, MFA, and data encryption.

Vetting

Many LEAs have vetting processes when contracting with a third party application. Some of these vetting processes go through departments in charge of curriculum or leadership and include discussion about educational efficacy, quality, but also can include reviewing the data requested, the data security and advocating for data minimization.

Catalysts for LEA Data Retention

Data Retention in Special Education Records

There is a drastic difference between retention of special education records and other records. Staff interviewed that managed special education records had clear retention schedules for those student records. Special education staff mentioned retention schedules for special education records in the form of physical papers, a network drive, and productivity suites.

Unlike retention for other records in LEAs, USBE explicitly trains special education directors on record retention. USBE has specific rules around special education records management, some of which are included in USBE Administrative Rule [R277-487](#), including a requirement that LEAs have special education retention schedules outlined in their policies and procedures. During annual special education directors training, USBE explicitly teaches about the applicable retention schedule and links to the DARS website.

In addition to explicit direction from USBE, the federal Individuals with Disabilities Education Act (IDEA) includes strict time frames around completing evaluations and reviewing Individualized Education Programs (IEPs). A familiarity with timelines surrounding records may contribute to special education staff knowledge and confidence in following retention schedules.

- One school-based staff member explained that each year they take one day in the summer to store and destroy special education records.
- One district administrator was only aware that special education had retention schedules and was not familiar with schedules for any other LEA records.

Storage Constraints

Many staff at LEAs who destroy data mentioned the catalyst for destroying the data was reaching storage limits. Instead of paying for more digital storage, or in an effort to clear physical storage space, they have been incentivized to begin to destroy records.

- A large school district began a new policy of deleting student productivity suite accounts 120 days after separation because their system began charging for storage.
- Another large school district has begun deleting student records when they run out of storage two to four years after separation.
- A large charter school staff member acknowledged that it was not a good policy to retain all data until they face storage restraints. But this has been their policy and now that they are facing additional storage costs, they would like to create a new policy.

Storage constraints are particularly poignant in the case study below.

Case Study: Security Footage

Three LEAs interviewed discussed their policies around retaining daily security footage. In one large LEA this included footage for 10 cameras on each bus as well as hallway cameras and cameras around the perimeters of each school.

Each of the three LEAs had policies that were mainly based on storage capacity. In two large school districts, security camera footage was retained for one month. In a small charter school, this footage was retained for two weeks.

This case study highlights the significant influence of storage capacity as a factor in data retention, even when extremely sensitive data is involved.

Obstacles to Data Retention

Data Needs

Many LEAs shared that they kept data just in case. There is a common sentiment among many staff members that keeping records for longer is the safest choice. One high school finance secretary shared that if they are not sure about a retention schedule, they keep the record longer “than we need to.” This perspective is commonly rooted in desires to be prepared with historical data for statistical analysis, to ensure that they have every piece of data that they are legally required to, and to ensure that they have data for former students.



Data Needs

Staff see reasons to retain data beyond scheduled limits.



Lack of Awareness & Clarity

Requirements and guidance aren't always known or easy to apply.



Competing Priorities & Resources

Time, staffing, and other priorities push retention lower.



Technological Constraints

Systems don't always support practical or automated retention.



“Too New” to Worry About It

Newer schools and staff may postpone addressing retention.



Unclear Responsibilities

Staff aren't always sure who owns retention work.

“We do tend to err on the safe side when it comes to retaining things.”

- Business Administrator

Data Analysis

Many LEAs shared that they need data that is scheduled for data retention, either to make data-driven decisions; to report to USBE; or to remain accountable for parents, employees, school boards, and other community members.

LEAs specifically cited attendance data to track chronic absenteeism and student performance year over year, although the relevant retention schedule directs to delete attendance records and class schedules after one year.

Case Study: Student Discipline Files

One charter school office specialist shared in an interview that their school had a number of students with significant behavior issues transfer to their school. However, very little behavior records were transferred with the students.

For one particular student with especially serious safety violations, the office specialist reached out to the previous school for information. The previous school told them that they did not have any of the student's discipline records anymore.

According to the applicable GRS, student discipline records ([GRS-15-4](#)) are to be retained, "until the resolution of the issue." The description of student misconduct includes conduct which "disrupts the educational environment, threatens or harms persons or property, or disrupts school activities."

This means a school may not have records of a transferring student's misconduct to share with another school. It could also be interpreted to mean that a school could not retain data internally on how many students had misconduct from one year to the next.

Following this retention schedule may also conflict with Utah Code [§ 53G-6-604](#) that was amended in 2026 to require that when a student transfers schools, the student record includes "the student's discipline file including any safe-school violation, reintegration, or threat assessment."

One large school district is using aggregated results and anonymized data to keep useful statistics to hold on to some data surrounding attendance. This requires a level of data expertise, staff time, and awareness of retention schedules that is not always present in other schools.

"It is a little bit of a security blanket having a lot of historical data."
- Charter School SIS Manager

Legal Protection

Another concern of some LEAs is a fear of destroying data that they are legally obligated to retain. If they are found to have improperly destroyed the data, they are concerned about legal ramifications.

"I'm afraid to delete what we should."
- IT programmer

For example, one large school district had started to destroy data methodically, attempting to follow a retention schedule. However, when a legal issue arose, they found that they had deleted needed data. They have since stopped following retention schedules and are retaining most student and employee data indefinitely.

A small school district IT director shared their concerns that if they delete records, it could appear like they were covering up incriminating evidence.

Former Students

Finally, LEAs use retained data to support former students.

In particular, three interviewed staff members mentioned using retained data to respond to requests from "downwinders," meaning people who lived in Utah during the testing of nuclear weapons between 1951 and 1962. Those with illnesses linked to radiation may receive compensation, but need proof of residence in locations where there was testing. To obtain that proof of residence, many reach out to their LEAs for documentation.

These concerns may be indicative of a lack of awareness of retention schedules and DARS resources, because DARS maintains permanent records after 40 years. Thus all downwinder records, which are between 62 and 75 years old, should be archived at the archives. In particular, a DARS staff member shared that they have structures in place specifically to support downwinders.

These LEA staff members may not be aware that they could ensure retention and support for former students while also following retention schedules by sending records to archives.

Lack of Awareness and Clarity

Lack of Awareness

"I did not know I needed to."

- School Nurse

General Data Retention

Some staff members, particularly school-based staff, were simply unaware of retention schedule obligations or unaware of the student data they created, stored and maintained.

- When asked about destroying records in their Google or Microsoft productivity suites, one school psychologist and one school nurse did not know there was a need.
- One school counselor explained that they do not manage retention schedules for their Google or Microsoft productivity suites because they did not have any student data. However, they shared later that they kept student letters of recommendation on their Google drive.

DARS

For many LEA staff members interviewed, there was no knowledge about the work or resources of DARS.

- A long-time SIS data manager from a medium sized school district, a district specialist, and a large charter network staff member had never heard of the DARS or any of their resources.
- A rural school nurse and large district specialist did not know they could send records to DARS.

Only two large school districts mentioned interacting with the DARS staff member that supports LEAs; none mentioned any on-site training, although DARS offers it upon request.

Despite offering permanent data retention storage for any format, of the LEA staff interviewed who were aware of DARS, none were aware that they could submit any records other than physical paper.

Lack of Clarity

“Without clarity, we just do not dare get rid of things.”

- District IT Director

“When I [talk] with other tech directors, this subject comes up every so often and everyone’s like ‘What do we do here? Where do we find the guidance we need?’”

- Technology Director

Without clear and specific guidance around data retention requirements, many LEAs do not feel confident enough to destroy data.

Current retention schedules do not align with modern LEA practices or data. Some record’s schedules are too specific, while others are too broad and cannot easily be applied. Worse still, some records are altogether missing from GRSs. Furthermore, even when appropriately specific GRSs do exist, they can be challenging to find and apply, as evidenced by the Lunch Tally Record Example below.

Case Study: Lunch Tally Records

One school shared their journey to find the appropriate retention schedule for a record of the number of students who were planning on eating school lunches. They consulted their USBE quick guide and then contacted their district ARO. Together they were not sure, but decided to retain these lunch records for 4 years.

As it turns out, a Lunch Tally Record GRS ([GRS-1535](#)) does exist and was established in 2018. According to this GRS, the lunch reports should be retained only until superseded. All AROs receive DARS training, but this one was still unable to find the proper retention schedule.

This case study demonstrates the errors in records retention that can occur with insufficient support and training for LEA staff, even despite LEA willingness to become compliant.

Even the few LEAs who communicate frequently with DARS and AROs who are trained by DARS, felt confused and unable to confidently apply retention schedules in their LEAs.

LEA-Created Retention Schedules

Districts, schools and charter schools may all work with DARS to create agency-specific record retention schedules. This can be done when an LEA does not feel that they have an existing general record retention schedule that fits their records. While this could be a helpful tool to allow LEAs to slowly improve the scope of record retention schedules, it can also add to the confusion of the records schedules.

For example, the following four similar records have overlapping topics, definitions, dates, and different retention schedules. More information about these records can be found on the [archives website](#).

Title	Agency	Dates	Retention	Disposition
Committee Minutes	Salt Lake City School District	1921-1953, 1977-2023	Permanent Retain until administrative need ends.	Transfer to Archives
Administrative Council Minutes	USB	1986-	Permanent. Retain for 3 years.	Transfer to Archives
Board Minutes and Policies	Navigator Pointe Academy	2005-	Permanent. Retain for 5 years.	Transfer to Archives
School Board Agenda	Salt Lake City School District	1986-	Retain for 2 years.	Destroy

Competing Priorities for Resources

"This is one of those many things that you don't always have the time, or the resources, or personnel , or, I'm not sure exactly what, but you don't have whatever you need to prioritize it."

- Rural IT Director

"No one has ever asked me to [destroy records]."

- Rural District SIS manager

"It is not mission critical."

- Medium-sized District SIS Manager

Some LEA staff members interviewed felt there was pressure from LEAs, USB, and the legislature for more data, not less. LEAs also have no obvious incentives to prioritize record retention as well as no perceived consequences to a lack of

retention compliance. As evidenced above in Data Needs, there may even be incentives for retaining records. Faced with other more pressing tasks, LEA data retention is deprioritized.

Lack of Time/Staff

“As a small district, we've got so many other things going on that it's just hard to find the time to sit down and actually look into [record retention schedules]....I'd say the biggest [obstacle] is just the guidance and a lack of time.”

- Appointed Records Officer

- For one school district's ARO, the process of preparing and sending records to the DARS demands time and, most critically, staff that they sometimes cannot spare.
- At one school, it took staff one week to organize, pack and shred papers when moving to a new building. During the process, a shredder was completely burned out.

Technological Constraints

Google and Microsoft Productivity Suite Obstacles to Data Retention

There is currently no simple way to track retention schedules in cloud-based Google and Microsoft productivity suites. IT staff can delete users, but it must be done manually. Documents can automatically be deleted, but only based on the last time they have been opened. A retention schedule that would require documents to be deleted by their type, creation, or use would be a difficult manual process currently.



There is currently **no** simple way to track retention schedules in cloud-based Google and Microsoft productivity suites.

SIS Obstacles to Data Retention

SISs are designed to manage operations, but often not designed with easy functionality for deleting data. Many LEA staff mentioned that even if they wanted to begin to delete information in an SIS that there is no automated way to do it with commercially-purchased SISs. Currently, deleting records would be an extremely manual and time-consuming process for SISs.

Currently, deleting records would be an **extremely manual and time-consuming process for SISs.**

- According to an SIS manager of a small district, it is a huge burden to delete data and not feasible at the volume collected by the LEA.
- At a large district, an IT director researched purchasing some tools that would more easily be able to scan through the volume of data to identify what would be eligible for destruction, but ultimately it was too expensive.

Third Party Data Retention Obstacles

Three LEA data managers who are responsible for DPAs mentioned that they struggle to know when third parties are no longer being used. Many LEAs have vetting or approval processes for contracting with a third party but no easy method of communicating with all potential teachers using an application to determine

when a contract is no longer in use. This makes it different to determine when it is time to request destruction of data from the third party.

Too New to Worry About Data Retention

“We haven’t deleted anything to this point because we’re so new. We probably need a plan before five years hits.”

- Charter School Staff Member

Whether new staff or new schools, many LEAs cited this as a reason for not yet grappling with data retention. However, many education records have retention schedules as short as one year or less for those records that should be retained “until an issue is resolved.”

- When asked about their data retention, a two, three, eight, and twelve year old school all explained that their school was too new to have to confront data retention yet.
- One front desk secretary in their fourth year and another staff member in their third year of work shared that they were too new in their positions to have confronted data retention.

Unclear Responsibilities within an LEA

Within an LEA, it is not always clear who is responsible for data retention. There is an ARO, but that person is often removed from the specifics of the creation or maintaining of records across an LEA.

- One ARO shared that there was a lack of clarity between a records person and a specialist in charge of particular records, like a transportation director.
- Some school-level staff believe that data retention does not apply to them and that it is the office or district’s job.

Recommendations

Due to the complexity of data retention schedules, a lack of guidance, misunderstandings, low prioritization, and technological obstacles, LEAs are not in compliance with retention schedules. Despite many LEAs being aware of this lack of compliance, they are not confident about what to do to get into compliance. Failing to manage data retention and destruction makes more data vulnerable in the event of a cyberattack and threatens student data privacy.

1. Modernize

Create a statewide set of education retention schedules

2. Support

Provide training and role-based resources

3. Clarify

Define ownership and responsibilities

The following recommendations are critical to ensuring that LEAs can begin the process of becoming compliant in data retention laws and implementing best practices.

The LEA members of the Data Systems and Reporting Advisory Committee voted to make the following recommendations.

Recommendation 1

Modernize Retention Schedules

The local education agency members of the Data Systems and Reporting Advisory Committee recommend that the current record retention schedules are reviewed and revised, with involvement from local education agencies, and adopt new general retention schedules relevant to all LEAs across the state.

Recommendation 2

Provide Resources and Training

The local education agency members of the Data Systems and Reporting Advisory Committee recommend that the revised set of education retention schedules is accompanied by the following support.

- **For any LEA staff that have access to any records:** Role-based resources and general retention training
- **For Appointed Records Officers:** education-specific training and regular collaboration meetings

Recommendation 3

Clarify Ownership and Responsibilities

All members of the Data System and Advisory Committee recommend that USBE, the Legislature, and the DARS clearly delineate ownership and responsibilities for LEAs, USBE, and DARS for creating and maintaining retention schedules and providing guidance and support.

Implementation Considerations

Fiscal Considerations

Revising current retention schedules relevant to public education and compiling them into a new set of retention schedules would require one full-time employee to work for a minimum of one year. On-going updates to the retention schedule, support and guidance costs would depend on the division of labor among LEAs, USBE and DARS.

Consolidated Set of New Retention Schedules

There are many issues with the current retention schedules available to LEAs.

The main resource available to LEAs, the RAMP, was created by compiling previously-created retention schedules for records. These have been added piecemeal over time and many do not fit with current records management practices or common LEA records.

Instead of continuing to create or update record retention schedules sporadically, an entire overhaul of education general record retention schedules is necessary.

Instead of continuing to create or update record retention schedules sporadically, an entire overhaul of education general record retention schedules is necessary.

The process of creating new retention schedules would require working with DARS to establish new retention schedules and identify and remove outdated ones. It would require working with many LEAs to discover what records they commonly create and ensure these are all accounted for clearly in records schedules. It would also require working with subject matter experts at the USBE, particularly as they

stay up-to-date on legislative changes that may impact retention schedules, such as new data collection requirements.

Once this new set of retention schedules is completed, all LEAs should be encouraged to adopt it. It may be best to remove school and district created agency-specific record schedules to promote the most clarity.

Resources and Training

“[Are you] going to come back and train us on all of this?”
- School Nurse

“I don't think that until such a thing exists that a lot of small districts will ever be able to really be compliant.”
- Rural IT Director talking about clear guidance for record retention

Once a new set of record schedules has been created, LEA roll out should include regular training and guidance.

Many LEA staff feel underqualified to confidently make decisions about data retention for general records, but special education records are different. This is, in part, because those who manage special education records have annual training, resources and are aware that support can be found within the USBE special education team. Training and guidance would boost awareness of data retention concerns, increase confidence and increase compliance.

In particular, training should be created that caters to all LEA staff who have access to records. Role-based resources should also be created, so that teachers, office staff, business administrators, LEA leaders, and other staff can access resources that are applicable to their subject matter expertise.

Agency Ownership

Ultimately there is confusion around responsibilities between USBE, DARS, and LEAs. Currently, primary responsibilities regarding data retention fall on LEAs.

When there are issues with education-specific retention schedules or when a new one needs to be created, LEAs must bring these to the attention of DARS and lead the work to make those changes. This is the case even when a GRS is required by legislation for all LEAs. This requires awareness, time, resources and expertise. It is also unclear to many LEAs that this is their responsibility. Some assume that



another entity with more relevant expertise would be responsible for updating retention schedules on their behalf.

As a result of USBE's previous support to LEAs on data retention and general close relationships with LEAs, many LEAs assume that USBE can provide guidance on data retention. However, currently there is no USBE staff responsible for supporting LEAs in data retention because there is no legal responsibility for LEAs to support retention. This responsibility lies with DARS.

While DARS offers services and trainings to LEAs, LEAs are not using DARS services. Those LEAs that do communicate frequently with DARS still do not find the guidance they need to feel confident and become compliant. DARS support every government entity and their staff have general retention expertise, but cannot always answer education-related records questions.

Clarity around ownership is critical for progress.

Whether USBE or DARS takes on the project of revising retention schedules and creating a new set of retention schedules for LEAS, this project must be completed before LEAs can be expected to be compliant in records retention.

Appendix

Appendix A: The Data System and Reporting Advisory Committee

In accordance with Utah Code [§ 53E-3-526](#) and under the guidance of USBE Board leadership, the Data Systems and Reporting Advisory Committee was formed with a variety of required stakeholders; however, all individuals with relevant interest and experience were invited to apply. Information and applications were emailed to subscribers on electronic mailing lists of LEA staff in May 2025. A panel of USBE staff reviewed and ranked all applications received. Members were selected based on their relevant experience and to ensure varied representation. The committee was finalized at the end of May and held its first meeting in early June 2025.

The committee has had a total of 24 members throughout its course. There are 15 members currently working in LEAs. Of these members, there is a mix of urban, rural, and charter LEAs represented. Four of Utah's six largest school districts—Davis, Jordan, Nebo, and Washington County—are represented on the committee. One committee member is an elected USBE board member, five are USBE staff members, and one is a representative from DARS.

Role	Appointed Individual
Representative from the Utah Division of Archives and Records Service	Maren Peterson
District or charter school technology director	- David Williams, <i>Davis</i> - Melisa Richardson, <i>Logan City</i>
District or charter school designated data manager	- Jim Black, <i>Washington County</i> - Caleb Olson, <i>Jordan</i> - Emily Bejarano, <i>Academica West (representing charter schools)</i>
District or charter school designated information security officer	Jason Eyre, <i>Murray</i>
District or charter school appointed records officer	- JaDean Frehner, <i>InTech Collegiate Academy Charter</i> - Stacie Gomm, <i>Cache County</i> - Scot McCombs, <i>Canyons</i>
District or charter school legal counsel	Ben Onofrio, <i>Davis</i>
District or charter school business administrators	Misty Biesinger, <i>Greenwood Charter</i>
Other	- Steven Harwood, <i>Jordan</i> - Eric Ferrin, <i>Nebo</i> - Jonathon English, <i>San Juan</i>
Utah School Superintendents Association/Utah School Boards Association Representative	Ben Dalton, <i>Kane County</i>
Board member of the USBE	Sarah Reale
USBE Deputy Superintendent of Policy	Elisse Newey
USBE Director of Privacy	Katy Challis
USBE Director of Data and Statistics	Aaron Brough
USBE IT Deputy Director	Jared Felt

Appendix B: Interview Questions

1. What is your position?
2. What types of student personally identifiable information (PII) do you collect?
3. What are the locations/formats that your LEA stores student PII?
4. Are you familiar with Data Retention Schedules?

The following questions were repeated for each format that data was stored (in Microsoft or Google productivity suites, as physical paper records, in personal LEA-issued devices, on network drives, in SIS, in third party applications or other)

Track Data Retention

1. Do you track data retention schedules for this format?
 - a. If so, how?
 - b. If not, why?
2. Do you dispose of outdated data for this format?
 - a. If so, how?
 - b. If not, why?
3. Do you ever keep a record of what you have disposed of?
4. Do you ever archive data by sending it to the Division of Archives?

Secure Stored Data/Access Control

1. What are the ways that you secure stored data for this format?

Appendix C: Compliance with Cybersecurity and Data Privacy

LEA Compliance with Privacy Requirements

Historically, USBE's student data privacy team has monitored LEA compliance with Utah Code 53E-9 through an annual privacy compliance review. LEAs submitted documents required of them by federal and state law to the student data privacy team, who reviewed them to ensure that requirements were met, and then returned them to the LEA for revision as necessary. Required documentation included the Family Educational Rights and Privacy Act (FERPA) Annual Notice of Rights, the Directory Information Notice, the Student Data Collection Notice, the Data Governance Plan, and the Metadata Dictionary. The results below show the percentage of LEAs who demonstrated compliance of each document at the end of the review period.

Compliance Document	2021	2022	2023	2024	2025
Annual Notice of FERPA Rights	96.8%	93.6%	93.6%	99.4%	96.1%
Directory Information Notice	95.5%	89.7%	91.0%	99.4%	98.7%
Student Data Collection Notice	96.1%	94.9%	95.5%	99.4%	88.9%
Data Governance Plan	93.5%	92.9%	92.3%	98.7%	88.9%
Metadata Dictionary	Not monitored	5.6%	58.4%	87.1%	85.6%

For the 2025-2026 school year, USBE switched to a goal-based model of monitoring, wherein LEAs complete a self-assessment, determine a goal area for the school year, receive needed support, and then report on the level of completion of their goal. As that model is based on meeting individual needs and does not establish a single threshold for compliance, results similar to those above do not exist.

LEA Compliance with Security Standards in USBE Administrative Rule

USBE does not monitor compliance with security standards outlined in the USBE administrative rules. Historically, USBE sent a survey to LEAs requesting information about their cybersecurity frameworks. However, this practice was suspended to determine and establish the shared responsibilities between LEAs, USBE, the Utah Education and Telehealth Network (UETN), and the Utah Cyber Center, in part as a result of [H.B. 44 School Security Personnel Standards](#).

There is information available through recent studies, which offer insight into LEA cybersecurity. After conducting testing and statewide surveys, a [performance audit](#) by the Office of the Legislative Auditor General (2025) found that LEAs could do more to meet baseline cybersecurity best practices. LEAs shared barriers to full cybersecurity implementation to be “insufficient staffing, limited resources, and lack of prioritization.” In a survey of 51 LEAs by the UETN, more than half of LEAs had not fully implemented MFA, patch management, exposure to the internet, incident response plans, and training (Office of the Legislative Auditor General, 2025).

Appendix D: Personally Identifiable Student Data

According to Utah Code [§ 53E-9-301](#)(15)(a) "Personally Identifiable Student Data" means "student data Information About a Student or Students' Family Members

Information About a Student or Students' Family Members

- First and last name
- Home or physical address
- Information that a person collects online and combines with other personally identifiable student data to identify a student

Information About a Student

- Email address
- Telephone number
- Social security number
- Biometric identifier
- Health or disability data
- Student identification number
- Social media user name and password
- Information that alone or in combination is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty
- A combination of a student's last name or photograph with other information that together permits a person to contact the student online

If Associated with Personally Identifiable Student Data

- A customer number held in a cookie
- A processor serial number

Appendix E: Necessary Student Data

“Necessary Student Data” in Utah Code 53E-9-301(12) Explicitly Includes
(including all data required by state code or federal law)

- Name
- Date of birth
- Sex
- Parent contact information/custodial parent information
- Contact information
- A student identification number
- Local, state, and national assessment results (or an exception from taking a local, state, or national assessment)
- Courses taken and completed, credits earned, and other transcript information
- Course grades and grade point average
- Grade level and expected graduation date or graduation cohort degree, diploma, credential attainment, and other school exit information
- Attendance and mobility
- Drop-out data
- Immunization record or an exception from an immunization record
- Race
- Ethnicity
- Tribal affiliation
- Remediation efforts
- An exception from a vision screening required under Section 53G-9-404 or information collected from a vision screening described in Section 53G-9-404
- Information related to the Utah Registry of Autism and Developmental Disabilities, described in Section 26B-7-115
- Student injury information
- A disciplinary record created and maintained as described in section 53E-9-306
- Juvenile delinquency records

Citations

Davis, D., John, K., Stock, L., Allan, S., Goodfellow, C., Kersey, M. (2023, August 3). Data Reliability Audit-Assessment Data Report 22-01-A. USBE Internal Audit. https://www.schools.utah.gov/internalaudit/_internalaudit/_auditreports/_20230803AssessmentData2201A.pdf

Davis, D., John, K., Stock, L., Allan, S., Goodfellow, C., Kersey, M. (2023, November 2). Data Reliability Audit-Graduation and Student Data Report 22-01-B. USBE Internal Audit. https://www.schools.utah.gov/internalaudit/_internalaudit/_auditreports/_20231030GraduationStudentData2201B.pdf

Office of the Legislative Auditor General. (2025, September). *A performance audit of public and higher education cybersecurity* (Report No. 2025-19). Utah State Legislature. <https://le.utah.gov/interim/2025/pdf/00003788.pdf>

U.S. Government Accountability Office. (2022, October). *Critical infrastructure protection: Additional federal coordination is needed to enhance K-12 cybersecurity* (Publication No. GAO-23-105480). <https://www.gao.gov/products/gao-23-105480>

Utah State Board of Education. (2025, September). *School data amendments report: Utah's student information systems*. <https://le.utah.gov/AgencyRP/reportingDetail.jsp?rid=777>