# DAVIS SCHOOL DISTRICT
# DATA GOVERNANCE PLAN
## STUDENT DATA PROTECTION

## Purpose

Data governance is an organizational approach to data and information management that is formalized as a set of policies and procedures that encompass the full life cycle of data; from acquisition, to use, to disposal. The Davis School District takes seriously its moral and legal responsibility to protect student privacy and ensure data security. Utah's Student Data Protection Act requires the District adopt a Data Governance Plan.

The Plan works in conjunction with a variety of District policies and procedures and is structured to encourage the effective and appropriate use of educational data; centering on the idea that data is the responsibility of all District schools and departments; and that data driven decision making guides what data is collected, reported, and analyzed.

## Collecting and Using Student Data

The District or school will collect students' personally identifiable information (PII) by lawful and fair means and, where appropriate, with the knowledge or consent of the individual concerned.

Before or at the time of collecting PII, the District or school will identify the purpose for which the information is being collected. We will collect and use students' personally identifiable information (PII) solely with the objective of fulfilling those purposes specified by us and for other compatible purposes, unless we obtain the consent of the individual concerned or as required by law. Personal data should be relevant to the purposes for which it is to be used, and, to the extent necessary for those purposes, should be accurate, complete, and up-to-date.

## Maintain and Protect Student Data

The District maintains an information technology security program that is updated at least annually. The program consists of annual security training, third-party risk assessments, security testing, and audits. District systems are updated regularly to prevent unauthorized access to our systems.

The District maintains a variety of policies and procedures that address data and information privacy which are intended to secure all media containing sensitive or confidential data.

## Data Security and Privacy Training

The District will provide a range of training opportunities for all District employees with access to student educational data in order to minimize the risk of human error and misuse of information.

Through the District electronic document signing process in Encore; District employees shall annually acknowledge review of District policies, privacy of student information, and the District's Employee Acceptable Use Agreement.

Supervisors will ensure employees receive proper training based on their individual roles and responsibilities in the organization to prevent unauthorized access and minimize the risk of data breaches.

The District shall make readily available to students, parents, and patrons information about our policies and practices relating to student PII.

## Sharing Student Data

Providing data to persons and entities outside the District increases transparency, promotes education in Utah, and increase knowledge about Utah public education.

The District or school will only share education records and/or personally identifiable information (PII) in accordance with federal and state student privacy laws, and as outlined in District policy 11IR-110 Family Educational Rights and Privacy Act.

De-identified data, aggregate data, or anonymized data that could not be used to identify a particular student is not considered personally identifiable and may be released without consent or authorization.

## Record Retention and Expungement

The District and its schools shall retain and dispose of student records in accordance with the District's adopted student records retention schedule. Student records not on the District schedule shall be retained and disposed of in compliance with active retention schedules for student records per the Utah Education Record Retention Schedule.

In accordance with Utah Code §53E-9-306, to ensure maximum student data privacy, the District shall, in accordance with Utah Board of Education rule, expunge student data that is stored, by the District. Student-level discipline data will be expunged in accordance with federal law (20 U.S.C. 7917), state law (UCA §53E-9-306), and Utah Board of Education rule.

## Data Auditing

The District Information Technology department performs regular and ad hoc data auditing. We analyze data in the warehouse for anomalies and investigate the source of the anomalies.

## Data Breach

The District shall follow industry best practices to protect information and data in the event of a data breach or inadvertent disclosure of personally identifiable information. Prompt response is essential for minimizing the risk of any further data loss and, therefore, plays an important role in mitigating any negative consequences of the breach, including potential harm to affected individuals.

If there is a release of a student's personally identifiable student data due to a security breach the District shall notify the student, if the student is an adult student; or the student's parent, if the student is not an adult student. (UCA §53E-9-304)

## Data Transparency

The District has established a metadata dictionary that shows clear ownership and stewardship of each data element being collected and how we use it.

## Contact Information

The District has designated an individual to act as a student data manager to authorize and manage the sharing, outside of the District, of personally identifiable student data from a cumulative record maintained by the District as described in UCA §53E-9-308; and to act as the primary local point of contact for the state student data officer described in UCA §53E-9-302.

Patrons who have questions, comments, or suggestions on Student Data Privacy issues may contact the student data manager:
Jon Hyatt
Assessment Department
(801) 402-5360
jhyatt@dsdmail.net

Data Advisory Team
IT Systems Security Manager – Ensures compliance with security systems laws, investigates complaints of alleged security violations and systems breaches.
Director of Assessment – Acts as the primary point of contact for external research request.
Legal Counsel – Acts as legal representative to ensure all procedures and policies comply with federal and state law.

# Student Data Protection

| GLOSSARY OF TERMS | |
|---|---|
| **Data breach** | Is any instance in which there is an unauthorized release or access of PII or other information not suitable for pubic release. This definition applies regardless of whether the District stores and managers it data directly or through a contractor, such as a cloud service provider. Data breaches can take many forms including: hackers gaining access to data through a malicious attach; lost, stolen, or temporary misplaced equipment; employee negligence; staff misconfiguring a security service or device; policy and/or system failure. |
| **Education records** | Include those records that are directly related to a student and are maintained by an educational agency or institution or by a party acting for the agency or institution. For more information, see the Family Education Rights and Privacy Act regulations, 34 CFR §99.3. |
| **Personally identifiable information** | Refers to information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. A list of what PII includes can be found in Utah Code Ann. §53E-9-301. |
| **School official** | Includes a person employed by the District as an administrator, supervisor, instructor, or support staff member; a person serving as a volunteer; a person serving the District School Board; a person or company with whom the District or school has contracted to perform a special task, or to whom the District has outsources institutional services or functions. |
| **Direct personal identifiers** | Include information that relates specifically to an individual such as the individual's name, address, Social Security Number or other identifying number or code, telephone number, e-mail address, or biometric record. |
| **Indirect personal identifiers** | Such as the name of the student's parent or other family members; the student's or family's address, date and place of birth, and personal characteristics or other information that would make the student's identity easily traceable. |
| **Directory information** | Includes information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. This District has identified the following as directory information: name, address, telephone number; date and place of birth; grade level and enrollment status; student's District email address; student's ID number that is displayed on a student ID badge; parent's email address; participation in officially recognized activities and sports; weight and height of members of athletic teams; dates of attendance; degrees, honor, and awards received; most recent previous educational agency or institution attended; and student's digital image. |
| **Limited use directory information** | The following shall be considered limited use directory information that may be disclosed only to other students enrolled in the same course(regardless of whether such students are enrolled in the same class section) that has been audio or video recorded by the District, for instructional and educational purposes only. Name to the extent it is referenced or captured during the audio or video recording; any photograph or image of the student captured during the audio or video recording; any audio or video recording of the student participating in the course; and any online chats or other recorded communications among participants in the course captured during the audio or video recording. |

## Sources for more detailed information

Privacy laws provide the baseline for data governance and privacy policies by establishing minimum protections for protecting students' personally identifiable information. These laws establish the definition of personally identifiable information (PII) and the guidelines surrounding the sharing of such information.

| Federal Laws | Description |
|---|---|
| Children's Internet Protection Act (CIPA) | Requires Internet safety policies such as technology to block certain access, and programs to educate students on appropriate online behavior. |
| Children's Online Privacy Protection Act (COPPA) | Assures that children under 13 years of age do not share personal information on the Internet without the express approval of their parents. |
| Family Educational Rights and Privacy Act (FERPA) | Affords parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records. |
| Military Recruiters – The Elementary and Secondary Education Act of 1965 (ESEA) | Requires local educational agencies receiving assistance under the ESEA to provide military recruiters with directory information (specifically names, addresses, and telephone listings) unless parents have opted out. |
| Protection of Pupil Rights Amendment (PPRA) | Establishes requirements related to parental notification and opt-out option when collecting information from students when administering surveys or physical exams/screenings. |
| Uninterrupted Scholars Act | Permits educational agencies to disclose a student's PII, without parental consent to a caseworker or other representative of a State or local child welfare agency when such agency is legally responsible for the student. Permits disclose pursuant to a judicial order without requiring additional notice to the parent by the educational agency in specified types of judicial proceedings in which a parent is involved. |

| Utah Laws | Description |
|---|---|
| Utah Family Educational Rights and Privacy Act | Protects the privacy of a student, the student's parents, and the student's family and supports parental involvement in the education of their children through compliance with the protections provided for family and student privacy under this part and FERPA. |
| Student Data Protection Act | An education entity or a third-party contractor who collects, uses, stores, shares, or deletes student data shall protect student data as described in this part. |
| Utah Administrative Code R277-484 Data Standards | The State Board is required to perform certain data collection related duties essential to the operation of statewide educational accountability and financial systems and to support the operation of required educational accountability and financial systems by ensuring timely submission of data by school districts. |

| Davis School District Policies | Description |
|---|---|
| 4I-005 Assessments of Student Achievement | To ensure that student progress is accurately measured through standardized achievement assessments, the District has developed a comprehensive assessment system plan in accordance with state and federal laws. Information from such student assessments may be used by the District, schools, and educators as an additional tool to plan, measure, and evaluate the effectiveness of the District's education program. |
| 7SS-001 Information Systems Security | Establishes requirements for use and protection of the District's network, computer and information systems, and the information transmitted via those systems. |
| 7SS-003 Technology Resources and Internet Safety | Establishes appropriate use of the technology resources provided to the District's employees, students, and parents for educational purposes. |
| 11IR-110 Student Data and Family Privacy Protection | Provides standards and procedures for the protection of private information within the curriculum and other activities; and in the administration of psychological or psychiatric examinations, test, or treatments, or any survey, analysis, or evaluation of students. |

| Other Resources and Information |
|---|
| Plan to Administer Statewide Assessments |
| Information Systems Security Standards and Procedures |
| Social Media Standards and Procedures |
| Elementary Student Acceptable Use Agreement |
| Secondary Student Acceptable Use Agreement |
| Employee Acceptable Use Agreement |
| Directory Information Notice |
| Family Education Rights and Privacy Act Guidance |
| Protection of Pupil Rights Guidance |
| Student Data Disclosure Statement |
| Third Party Vendors Review Procedures<br>Memorandum of Understanding to Share Students' PII<br>Data Privacy Agreement |
| FERPA Compliance U.S. Department of Education |