Granite School District
Technology Governance Plan

Table of Contents

Decision Making Authority

The Granite School District system provides different levels of data governance working together to ensure a system of checks and balances within the district. This hierarchy begins with the Data Governance Committee which oversees the program with direction from the Utah State Board of Education, revising and updating the policies as needed. The Director of Information Systems/Data Security Officer interprets the policies for the district and helps to ensure state and federal guidelines are being followed. Data stewards are responsible for implementing data governance policies and standards and maintaining data quality and security. Permission levels are assigned by the data stewards to ensure that access of information is limited to the scope of each person's job duties. Data stewards have the authority to quickly and efficiently correct data problems while still ensuring that their access to personally identifiable information (PII) is maintained in order to protect privacy and confidentiality. Granite School District data stewards include district program directors and school administrators who oversee the accuracy and security of their schools, or program's data.

Organization Structure

The Granite School District Data Governance Committee consists of Superintendent Designee; Mr. Dale Roberts, Director, Information Systems; Dr. Robert Averett, Director of Student Assessment; Mr. Douglas Larson, Director, Policy and legal services; Mr. Chris Larsen, Director Educational Technology; Mr. Todd Braeger, Director, Research and Evaluation; Ms. Noelle Converse, Director, Special Education; Ms. Charlene Lui, Director, Educational Equity; Ms. Donnette McNeill-Waters, Director, Human Resource; Ms. Leslie Bell, Director, Curriculum and Instruction; and Ms. Judy Petersen, Director, College and Career Readiness.

The Data Governance Committee shall meet annually at a minimum. Additional meetings shall be called as needed. The Data Governance Committee is responsible for formulating the data governance policies and procedures for the Granite School District.

Data Stewards/Roles and Responsibilities

The following chart indicates the data stewards who are assigned to areas of data responsibility along with their general roles and responsibilities. Data stewards are responsible for actively monitoring data-related activities for compliance with the established policies and procedures. Lists of data responbiltiels data stewards may not be exhaustive

Data	Steward	Role & Responsibility
Discovery (SIS) grades, schedules, demographic, special services, attendance, discipline	Director of Information Systems	Liaison between GSD & USBE on data reporting.

Assessment & Testing: School City, SAGE, ACT	Director of Student Assessment	Oversees the assessment of statewide and district formative testing.
Special education data (Goal view)	Director of Special Education	Oversee the records as it pertains to special education students
Educational Equity: ELL associated data, Title IX, OCR	Director of Educational Equity	Oversee the records of English language learner students
Online Curriculum (DIBELS, Wonders, Digits….)	Director of Curriculum & Instruction	Works with vendors on the iteration of student information for the purpose of classroom textbooks.
School Data	School Administrators	Oversee the proper use of applications and student data at the school/teacher level.
Canvas/classroom apps	Director of Educational Technology	Works to find the proper teacher tools to use in the classroom and students.
Human resources data	Director of Human Resources	Oversee the proper use and protection of all GSD staff records.
Student school classroom support information	Director College and Career Readiness	Oversees the proper use of support staff logs also teacher classroom behavior information.

Standard Policy and Procedures

Granite School District has the following administrative memoranda for student records.

045 – Student Records: Privacy of student records, Access to student records, Correction of student records, Disclosure of education records, Notice of rights: http://www.graniteschools.org/legal/wp-content/uploads/sites/22/2015/02/045-Student-Records.pdf

073 – Management of student records: maintenance, retention, release of records, transfer of records: http://www.graniteschools.org/legal/wp-content/uploads/sites/22/2015/01/073-Manage-Student-Records.pdf

Sustainability

To minimize the risk of human error and misuse of information, Granite School District will provide a range of training opportunities for all school district staff, including volunteers, contractors and temporary employees with access to student educational data or confidential educator records.

All GSD employees and contracted partners must sign and obey the districts **Employee Computer Use Agreement** which describes the permissible uses of district technology and information. New GSD employees must sign the aforementioned document prior to being granted access to GSD systems. All employees will be required to participate in **Data security and privacy fundamentals** training, which is mandatory for continued access to the GSD network. The signed agreement is maintained in the employee's electronic employee file. Non-compliance with the agreements shall result in consequences up to and including removal of access to GSD's network; if this access is required for employment, employees and contractors may be subject to dismissal (Termination).

Monitor Data Compliance

Compliance with federal and state mandates is of utmost importance. Granite School District Data Governance Committee will ensure the district abides by all laws and contractual obligations affecting its information systems including but not limited to the following:

FERPA, The Family Educational Rights and Privacy Act, protects the privacy of student records. Generally, Granite School District requires written permission from the student parent/guardian or from an eligible student to release information from a student's educational record. However, FERPA allows schools to disclose those records, without consent, to school officials with legitimate educational interest. Schools may share basic "directory" information such as students names and addresses if they give parents the opportunity to opt out. However, written permission is required to release all other information that would enable a member of the school community to identify the student. If parents/students find any erroneous data, they may present corrections to the local school officials who will correct such information with appropriate documentation. Parents should refer to Administrative Memorandum #45 regarding the release of directory information and FERPA.

CIPA, the Children's Internet Protection Act, was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the internet. CIPA imposes certain requirements on schools or libraries that receive discounts for internet access or internal connections through the E-rate program. Schools subject to CIPA have two additional certification requirements: 1) their Internet safety polices must include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness and response.

COPPA, the Children's Online Privacy Protection Act, regulates operators of commercial websites or online services directed at children under age 13 that collect or store information about children. Parental permission is required to gather certain information; see www.coppa.org for details.

HIPPA, the Health Insurance Portability and Accountability Act, applies to organizations that transmit or store Protected Health Information (PHI). It is a broad standard that was originally intended to combat waste, fraud, and abuse in health care delivery and health insurance but is now used to measure and improve the security of health information as well.

External Research

Research can be done for or on behalf of Granite School District if for an educational purpose under the studies exception of FERPA with the following guidelines.

FERPA outlined study exceptions

- Study purpose is to develop, validate or administer predictive tests.
- Validate the validity of student aid programs
- Improve Instruction

Written agreement must be in place for the purpose of the study that outlines.

  - Purpose, scope and duration of the study
  - What data are to be shared
  - Data can only be used for the purpose of the study
  - Data must be destroyed at the end of the study or at the request of Granite School District.

Research data should only be obtained through Granite School District. Datasets for external research should have all matching of student records and PII removed before releasing to any external entities.

All 3rd party partners obtaining or utilizing student information shall enter into a data sharing agreement that follow the FERPA exceptions outlined.

Data Inventories

Granite School District collects individual student data directly from students and/or families through its student data management system. Local student data is transmitted frequently to the state UtreX data collection system. Each student is assigned a unique student identifier upon enrollment into the student management system to ensure compliance with the privacy rights of the student and his or her parents/guardians.

Maintaining a complete up-to-date inventory of all records and data systems, including those used to store and process data, enables Granite School District to target its data security and privacy management efforts to appropriately protect sensitive data. The data records inventory specifies what data elements are collected, provides a justification for their collection and explains the intended purpose(s) for their use.

Student data Files: High Risk (HR) Medium Risk (MR) Low Risk (LR)

Low Risk Data Elements Collected
Student First/last name Student address Phone Grade level School attending Activity Information
Student Medium Risk Information
Attendance Schedule/course information Assessments Grades Transcript
Student High Risk Information
Health Immunization Medical Discipline Behavior Counselor logs Education equity Special Education Lunch

Data Content Management

All data elements are classified by their sensitivity levels. The committee evaluates the risk of disclosure of PII; potential for adverse effects for the individual should the data become compromised; and legal requirements to protect the data. The Data Security Officer ensures the appropriate security efforts are applied to protect the data.

Inventory of Software and Hardware

Granite School District maintains an inventory of hardware in its LANDesk management system. GSD employs Cisco's Identity Service Engine software (ISE) to manage all devices connected to either their wired or wireless network. All connected devices must have an approved profile to be allowed on the network. Granite School District maintains a software approval list that is supported by a software approval workflow process. This process involves the review of software by curriculum specialists as to how the software aligns with the Utah core standards or is a useful productivity tool. The software is also reviewed by Information Systems for system compatibility.

Access to Data Inventory

Granite School District maintains reports that outline staff access to student information as part of its Student Information System. The report shows what student information is accessible by groups and individual users. Access to the various areas of student records is categorized as read only or update (delete). The report is run and distributed annually to each school and department administrator for review. The administrator has the responsibility to review each staff member's access and send any corrections to Information Systems to adjust.

Data Records Management

Granite School District staff (as defined in Section 53A-1-1402(10)) shall retain and dispose of student records in accordance with Sections 63G-2-604 and 53A-1-1407, and comply with active retention schedules for student records per Utah Division of Archives and Records Service.

Granite School District follows the expungement practices outline in board rule 53E-9-306. Using and expunging student data.

Granite School District may create and maintain a cumulative disciplinary record for a student.

Data Quality

A proactive approach to data governance requires establishing data quality standards and regularly monitoring and updating the data management strategies to ensure that the data are accurate, relevant, timely, and complete for their intended purposes. To ensure high quality data, the following strategies are used to prevent, and correct errors and misuses of data.

1. Data stewards or their designees review student information for accuracy as parents, students and teachers submit it.
2. Data stewards or their designees correct data immediately when errors are brought to their attention.
3. Data stewards or their designees allow access to only those individual's with a "need to know" status as determined by the data stewards.

Data Access

The Granite School District holds data privacy, confidentiality, and security practices in the highest regard. All student data utilized by GSD is protected as defined by the Family Educational Rights and Privacy Act (FERPA) and Utah statute. This document outlines the manner in which GSD staff are to utilize data and protect personally identifiable and confidential information. A signed agreement form is required from all GSD staff to verify commitment to adhere to/abide by these practices. Failure to adhere to guidelines may result in personnel action, up to and including termination.

Appendix C references the Data Sharing and confidentiality agreement each employee will be required to acknowledge at the start of each school year.

Exchanging Data with External Entities

Ensuring that data dissemination activities complies with federal, state, and local laws is a key organizational responsibility. The release or sharing of any data without written consent must adhere to the polices and regulations established by Granite School District including procedures for protecting PII when sharing with other agencies and disclosure avoidance procedures for protecting PII from disclosure in public reports.

Student data is shared with certain external entities who contract with Granite School District. GSD is required by the Utah State Board of Education to disclose the data shared outside the district in the data dictionary provide in their data gateway. The disclosure of the data can be publicly viewed at https://datagateway.schools.utah.gov/DataDictionary/Home .

No school or department shall enter into a contract for the use of any program that requires the import of District data without first consulting and receiving approval from the district Data Security Officer. The officer will determine that appendix B &C are addressed as part of the district terms and conditions agreement with the vendor.

Physical Data Security and Risk Management

Data collected by the Granite School District is maintained within multiple secure infrastructure environments located within the district. Access to data is limited to pre-identified staff members who are granted clearance related to their job responsibilities of student management, federal reporting, program assessment, and policy development.

A. Responsibilities:
    a. The Director of Information Systems shall implement, maintain, and monitor technical access controls and protections for the data stored on the system's network.
    b. District employees shall not select or purchase software programs that will utilize or expose high risk data without first consulting the Data Security Officer

to determine whether or not adequate controls are available with the application to protect data.

c. The Information Systems staff will provide training for authorized users on how to properly access data to which they have rights.
d. Technical controls and monitoring cannot ensure with 100% certainty that no unauthorized access occurs. For instance, a properly authorized user leaves their workstation when logged in, and an unauthorized person views the data in their absence. Therefore, it is the shared responsibility of all employees to cooperatively support the effectiveness of the established technical controls through their actions.

B. Location of Data and Physical Security
    a. High risk data shall be stored on servers/computers which are subject to network/workstation controls and permissions.
    b. Servers storing sensitive information shall be operated by the Information Systems Department in compliance with all security and administration standards and policies.
    c. All servers containing system data will be located in a secure data center with limited access.
    d. District staff who must print reports that contain high or medium risk data shall take responsibility for keeping this material in a secured location – vault, locked file cabinet, etc. In addition, all printed material containing high-risk documentation shall be shredded when no longer in use.
C. Application of Network and Computer Access permissions
    a. The Information Systems Department shall be responsible for implementing network protection measures that prevent unauthorized intrusions, damage and access to all storage and transport mediums; including but not limited to:
        i. Maintaining firewall protection access to the network and/or workstations.
        ii. Protecting the network from unauthorized access through wireless devices, including establishing 'guest' wireless networks with limited network permissions.
        iii. Implementing virus and malware security measures throughout the network and on all portable computers.
        iv. Applying all appropriate security patches to servers and workstations.
        v. Establishing and maintaining password policies and controls on access to the network, workstations, and other data depositories.

Data Governance Training

Training in data security and student privacy laws is provided to specific individuals by the District Policy & Legal Services Department on a yearly basis. Staff will also sign a Data Sharing

Confidentiality Agreement for the assurance of confidentiality and privacy which is kept as part of the employee's electronic file.

Breach Notification

See Breach Practice Document in appendix.