NEBO SCHOOL DISTRICT
DATA GOVERNANCE PLAN

SECTION: ADMINISTRATION
TITLE: DATA GOVERNANCE PLAN

TABLE OF CONTENTS

1. PURPOSE AND SCOPE
2. DEFINITIONS
3. INFORMATION TECHNOLOGY SYSTEMS SECURITY PLAN
4. TRAINING, TECHNICAL ASSISTANCE, AND AUDITING
5. STUDENT DATA DISCLOSURE
6. EXPUNGING DATA

1. PURPOSE AND SCOPE

1.1. This Data Governance Plan (the "Plan") is adopted to comply with requirements found in Utah Code Title 53E, Chapter 9, Student Privacy and Data Protection. As set forth in Nebo School District Policy JO, *Student Records*, which was adopted before passage of the statutory requirements, the District has long taken seriously its moral and legal responsibility to protect student privacy and ensure data security.

1.2. Data governance is an organizational approach to data and information management that is formalized in this Plan as a set of law- and policy-based procedures encompassing the full life cycle of data—from acquisition, to use, to disposal. This Plan applies to all employees, including temporary employees and independent contractors. The Plan must also be used to assess the risk of conducting business with third parties, and all agreements in which data may be disclosed to third parties must be in compliance with this Plan.

1.3. In accordance with District policy and procedures, this Plan will be reviewed and adjusted on at least an annual basis. The Plan aims to accomplish the following statutory requirements:

1.3.1. incorporate reasonable data-industry best practices to maintain and protect student data and other education-related data;

1.3.2. provide for necessary technical assistance, training, support, and auditing;

1.3.3. describe the process for sharing student data between an education entity and another person; and

1.3.4. describe the process for an adult student or parent to request that data be expunged.

2. DEFINITIONS

2.1. "Access" means to directly or indirectly use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, computer network, or any means of communication with any of them.

2.2. "Authorization" means the express or implied consent or permission of the owner, or of the person authorized by the owner to give consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission.

2.3. "Computer" means any electronic device or communication facility that stores, retrieves, processes, or transmits data.

2.4. "Computer system" means a set of related, connected or unconnected, devices, software, or other related computer equipment.

2.5. "Computer network" means the interconnection of communication or telecommunication lines between: computers; or computers and remote terminals; or the interconnection by wireless technology between: computers; or computers and remote terminals.

2.6. "Computer property" means electronic impulses, electronically produced data, information, financial instruments, software, or programs, in either machine or human readable form, or any other tangible or intangible item relating to a computer, computer system, computer network, and copies of any of them.

2.7. "Confidential," when applied to data, text, or computer property, means protected by a security system that clearly evidences that the owner or custodian intends that it not be available to others without the owner's or custodian's permission.

2.8. "Data breach" means an unauthorized release of or unauthorized access to personally identifiable student data that is maintained by the District.

2.9. "Encrypted" means altered or converted into a cipher or code to conceal data in a way that requires a secret key or password to be decrypted, or converted back to an original readable format.

2.10. "Personally identifiable information (PII)" means data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

2.11. "Security system" means a computer, computer system, network, or computer property that has some form of access control technology implemented, such as encryption,

password protection, other forced authentication, or access control designed to keep out unauthorized persons.

2.12. "System level" means access to the system that is considered full administrative access and includes operating system access and hosted application access.

3. INFORMATION TECHNOLOGY SYSTEMS SECURITY PLAN

3.1. Consistent with the SDPA, this Plan "incorporates reasonable data industry best practices to maintain and protect student data and other education-related data." UTAH CODE ANN. § 53E-9-301(7)(a) (2018). Such practices are set forth in this section, which is the District's Information Technology Systems Security Plan ("IT Security Plan") required by UTAH ADMIN. CODE r277-487-3(14) (2017).

3.2. Data loss can be caused by human error, hardware malfunction, natural disaster, security breach, or other means and is not always preventable. The District strives to maintain network security, including security for all personally identifiable information, whether stored on paper or digitally on District-maintained computers and networks. This IT Security Plan provides procedures to mitigate threats that may cause harm to the district, its students, or its employees.

3.3. IT Security Officer

The Coordinator of Technical Services is hereby appointed the District IT Security Officer (ISO). The ISO oversees District-wide IT security, contributes to the development of data protection policies, and monitors adherence to the standards and procedures set forth in this IT Security Plan.

3.4. Physical Security

3.4.1. Computer Security

3.4.1.1. Employees must not leave computers unattended and unlocked, especially when logged into systems or programs that may display student or employee PII. Employees should use an automatic log off, locks, and password screen savers to ensure compliance with this requirement.

3.4.1.2. Employees shall ensure that all equipment that contains sensitive information is secured to deter theft.

3.4.2. Server/Network Room Security

3.4.2.1. The ISO shall ensure that server and telecommunications rooms are protected by appropriate access controls that segregate and restrict access from general school or District office areas. Access control shall be enforced using either keys, electronic card readers, or similar methods. Only those employees who need it to perform their job functions may be granted access.

3.4.2.2. Telecommunications rooms may only remain unlocked or unsecured if the building design makes it impossible to do otherwise or environmental factors require the door to be opened.

3.4.3. Contractor Access

3.4.3.1. Before any contractor is allowed access to any computer system, server room, or telecommunications room, the contractor must present a company-issued identification card, and his/her access must be confirmed directly by the authorized employee who issued the service request or by the ISO or his/her designee.

3.5. Network Security

3.5.1. Network perimeter controls will be implemented to regulate traffic moving between trusted internal (District) resources and external, untrusted (Internet) entities. All network transmission of sensitive data should enforce encryption where technologically feasible.

3.5.2. Network Segmentation

3.5.2.1. The Technical Services Department shall ensure that all untrusted and public access computer networks are separated from main district computer networks and utilize security policies to ensure the integrity of those computer networks.

3.5.2.2. The Technical Services Department will utilize industry standards and current best practices to segment internal computer networks based on the data they contain. This will be done to prevent unauthorized users from accessing services unrelated to their job duties and minimize potential damage from other compromised systems.

3.5.3. Wireless Networks

3.5.3.1. No wireless access point shall be installed on the District's computer network that does not conform to current network standards as defined by the ISO.

3.5.3.2. The Technical Services Department shall scan for and remove or disable any rogue wireless devices on a regular basis.

3.5.3.3. All wireless access networks shall conform to current best practices and shall utilize, at minimum, WPA encryption for any connections. Open access networks are not permitted, except on a temporary basis for events when deemed necessary.

3.5.4. Remote Access

3.5.4.1. The Technical Services Department shall ensure that any remote access with connectivity to the District's internal network is achieved using the District's centralized VPN service that is protected by multiple factor authentication systems. Any exception to this practice must be due to a service provider's technical requirements and must be approved by the ISO.

3.6. Access Control

3.6.1. System and application access will be granted based upon the least amount of access to data and programs required by the user in accordance with a business need-to-have requirement.

3.6.2. Authentication

3.6.2.1. The Technical Services Department shall provide strong password management for employees, students, and contractors.

3.6.2.2. Password Protection

3.6.2.2.1. Employees should not share their passwords with anyone except IT staff who need the password to help the employee with an access or other IT concern. All passwords are to be treated as sensitive, confidential information.

3.6.2.2.2. Passwords may not be disclosed on questionnaires or security forms.

3.6.2.2.3. Except when Technical Services staff are providing temporary or initial passwords, employees should not disclose hints that may reveal a password (for example, "my family name").

3.6.2.2.4. Any user suspecting that his/her password may have been compromised should change the password. If data appears to have been lost or stolen, the user should notify the ISO.

3.6.3. Authorization

3.6.3.1. The Technical Services Department shall ensure that user access is limited to those specific access requirements necessary to perform the user's job. Where possible, the District may segregate duties to control authorization access.

3.6.3.2. The Technical Services Department shall ensure that a user's access is granted or terminated promptly upon receipt, and ISO approval, of a documented access request/termination.

3.6.4. Accounting

The Technical Services Department shall ensure that audit and log files are maintained for at least ninety days for all critical security-relevant events such as invalid logon attempts, changes to the security policy/ configuration, failed attempts to access objects by unauthorized users, etc.

3.6.5. Administrative Access Controls

3.6.5.1. The District shall limit IT administrator privileges (operating system, database, and applications) to the minimum number of staff required to perform these sensitive duties.

3.7. Data Breach

3.7.1. Monitoring and responding to a data breach will be designed to provide early notification of events and rapid response and recovery from internal or external network or system attacks.

3.8. Business Continuity

3.8.1. To ensure continuous critical IT services, Technical Services will develop a business continuity/disaster recovery plan appropriate for the size and complexity of District IT operations.

3.8.2. The Technical Services Department shall develop and deploy a district-wide business continuity plan, which should include at a minimum:

3.8.2.1. Backup Data: Procedures for performing routine daily/weekly/monthly backups and storing backup media at a secured location other than the server room or adjacent facilities. At a minimum, backup media must be stored off-site a reasonably safe distance from the primary server room.

3.8.2.2. Secondary Locations: Identify a backup processing location, such as another School or District building.

3.8.2.3. Emergency Procedures: Document a calling tree with emergency actions to include: recovery of backup data, restoration of processing at the secondary location, and generation of student and employee listings for ensuring a full head count of all.

3.9. Malicious Software

3.9.1. Server and workstation protection software will be deployed to identify and eradicate malicious software attacks such as viruses, spyware, and malware.

3.9.2. The Technical Services Department shall install, distribute, and maintain spyware and virus protection software on all district-owned equipment, i.e. servers, workstations, and laptops.

3.9.3. The Technical Services Department shall ensure that malicious software protections include frequent update downloads (at least weekly), frequent scanning (at least weekly), and active malicious software protection (real time) on all operating servers/workstations.

3.9.4. The Technical Services Department shall ensure that all security-relevant software patches are applied to servers monthly and that critical patches are applied as soon as possible.

3.9.5. Computers should be equipped with anti-virus protection.

3.10. Internet Content Filtering

3.10.1. In accordance with federal and state law, the Technical Services Department shall filter internet traffic for content defined in law that is deemed harmful to minors.

3.10.2. The District acknowledges that technology-based filters are not always effective at eliminating harmful content. To mitigate the fallibility of filters, the District uses a combination of technological and supervisory means to protect students from harmful online content.

3.10.3. In the event that students take devices home, the Technical Services Department will provide a technology-based filtering solution for those devices. However, the District will rely on parents to provide the supervision necessary to fully protect students from accessing harmful online content.

3.10.4. Students shall be supervised when accessing the internet and using District-owned devices on school property.

3.11. Security Audit and Remediation

3.11.1. The Technical Services Department shall perform routine security and privacy audits.

3.11.2. The Technical Services Department shall develop remediation plans to address identified lapses.

4. TRAINING, TECHNICAL ASSISTANCE, AND AUDITING

4.1. Consistent with Utah law, this Plan "provides for necessary technical assistance, training, support, and auditing." UTAH CODE ANN. § 53E-9-301(7)(c) (2018).

4.2. The District will provide training on FERPA; Utah Code Title 53E, Chapter 9, Student Privacy and Data Protection; and District policies related to computer use, records management, and student records. All employees, volunteers, and independent contractors who have access to student PII must complete the training before using District networks

or electronic devices. The training may be incorporated into the District's annual Critical Policies training.

4.3. All employees and independent contractors must sign the Computer Use Agreement, which describes the permissible uses of District technology and information. Electronic signatures or other verification of agreement by employees after logging in to the Employee Portal constitute signature of the agreement.

4.4. Participation in the training will be monitored by supervisors.

5. STUDENT DATA DISCLOSURE

5.1. Consistent with Utah law, the District Superintendent will "designate an individual to act as the student data manager." UTAH CODE ANN. § 53E-9-303(2)(a) (2018). Consistent with USBE rule, the student data manager "authorizes and manages the sharing of student data; acts as the primary contact for the [state] Chief Privacy Officer; maintains a list of persons with access to personally identifiable student information; and is in charge of providing annual [District] training on data privacy." UTAH ADMIN. CODE r277-487-2(16) (2017). This Plan "describes the process for sharing student data between [the District] and another person." UTAH CODE ANN. § 53E-9-301(7)(d) (2018). Student PII may be shared only in accordance with FERPA and Nebo School District Policy JO, *Student Records*.

5.2. Access By Parents

5.2.1. Parents generally have a right to inspect and review the education records of their children. Access to the education records of a student who is or has been in attendance at a school in the District shall be granted to the parent of the student who is a minor or who is a dependent for tax purposes.

5.2.2. The school shall presume that each parent, regardless of custody designation, has authority to inspect and review their student's records unless the school has been provided a copy of a court order, state statute, or other legally binding document that specifically revokes these rights.

5.2.3. A parent's right to inspect and review his or her student's education record includes the right to access attendance records, test scores, grades, psychological records, applications for admission to other schools/colleges, and health or immunization information.

5.2.4. If material in the education record of a student includes information on another student, only the portion of the material relating to the student whose records were requested may be inspected and reviewed.

5.3. Access By Students

5.3.1. Notwithstanding the rights afforded to parents, students in Nebo School District may also inspect and review their own educational record in accordance with procedures set forth by the school that maintains the records.

5.3.2. When a student reaches eighteen (18) years of age or is attending an institution of post-secondary education, the rights accorded to, and consent required of, parents transfer from the parents to the student.

5.4. Access By School Officials

5.4.1. School officials who have a legitimate educational interest in a student's education record may access the record without parental consent.

5.4.2. For the purpose of this Plan, "school officials" shall mean any employees, trustees, or agents of the District, or of facilities with which the District contracts for placement of students with disabilities. The term also includes attorneys, consultants, and independent contractors who are retained by the District, or by facilities with which the District contracts for placement of students with disabilities.

5.4.3. School officials have a legitimate educational interest in a student's records when they are working with the student, considering disciplinary or academic actions, reviewing an individualized education program (IEP) for a student with disabilities, compiling statistical data, or investigating or evaluating programs that may involve the student.

5.5. Access By Other Persons

5.5.1. Personally identifiable information in education records shall not be released, except to the following:

5.5.1.1. Individuals for whom the parent has given written consent. Parents should use the District Consent to Release Educational Records of Student form.

5.5.1.2. School officials, including teachers, who have legitimate educational interests.

5.5.1.3. Officials of other schools, school systems, or institutions of postsecondary education in which the student seeks or intends to enroll, or where the student is already enrolled so long as the disclosure is for purposes related to the student's enrollment or transfer.

5.5.1.4. Authorized representatives of the Comptroller General of the United States, the Secretary of Education, or state and local educational authorities who require access to student or other records necessary in connection with the audit and evaluation of federal or state supported education programs or in connection with the enforcement of or compliance with federal legal requirements that relate to such programs.

5.5.1.5. Personnel involved with the student's application for, or receipt of, financial aid.

5.5.1.6. Organizations conducting studies for educational agencies or institutions for the purpose of developing, validating, or administering predic-

tive tests, administering student aid programs, and improving instruction. Such studies must be conducted so that personal identification of students and their parents will not be revealed to persons other than authorized personnel of the organizations conducting the studies.

5.5.1.7. Accrediting organizations that require the information for purposes of accreditation.

5.5.1.8. Parents of a student who is a dependent for tax purposes.

5.5.1.9. The student.

5.5.1.10. Individuals authorized by a judicial order or lawfully issued subpoena.

5.5.1.11. Appropriate persons who, in an emergency, must have such information in order to protect the health or safety of the student or other person.

5.5.1.12. Persons or organizations authorized by the school's administration to obtain directory information.

5.5.1.13. An agency caseworker or other representative of a state or local child welfare agency who provides documentation showing the right of that caseworker or representative to access the particular student's case plan. If shared with the Department of Human Services, the Department must be legally responsible for the care and protection of the student or providing services to the student. The student's PII may not be shared with a person who is not authorized to address the student's education needs. Consistent with UTAH CODE ANN. § 53E-9-308(4) (2018), a school official may share personally identifiable student data to improve education outcomes for youth:

5.5.1.13.1. in the custody of, or under the guardianship of, the Department of Human Services;

5.5.1.13.2. receiving services from the Division of Juvenile Justice Services;

5.5.1.13.3. in the custody of the Division of Child and Family Services;

5.5.1.13.4. receiving services from the Division of Services for People with Disabilities; or

5.5.1.13.5. under the jurisdiction of the Utah Juvenile Court.

5.5.2. The parent shall provide a signed and dated written consent before the school discloses personally identifiable information from a student's education records to any individual, agency, or organization other than the parent, the student, or those listed above. Such consent shall specify records to be released, the reason for such release, and to whom the records are to be released. Parents should use the District Consent to Release Educational Records of Student form.

5.6. Employees may not share student PII during presentations, webinars, or trainings. If an employee needs to demonstrate child/staff level data, demo records should be used rather than actual student PII.

5.7. Employees must redact all student PII from any document that is shared with a general audience.

5.8. Employees must take steps to avoid disclosure of student PII in reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.

5.9. Consistent with UTAH CODE ANN. § 53E-9-303(4) (2018), the District has established the following process for a request for data for the purpose of external research or evaluation. Student PII may not be shared for the purpose of external research or evaluation.

5.9.1. All student data requests for purposes of external research or evaluation must be submitted to the Curriculum Coordinator.

5.9.2. The Curriculum Coordinator will ensure the proper data are shared with external researchers or evaluators to comply with federal, state, and board rules.

5.9.3. Prior to conducting research or surveys in Nebo School District, approval must be obtained from the District Curriculum Staff Committee.

5.9.4. In order to conduct research or implement a survey, a Research Project Application must be completed and submitted to the Curriculum Coordinator.

5.9.5. Research Project Applications must be accompanied by a project proposal and must include a copy of the instruments that will be used.

5.9.6. Research projects that require the participation of teachers and/or students during the first thirty days or the last thirty days of the school year will generally not be approved.

5.9.7. Research proposal approval will generally be limited to those projects that complete the requirements associated with a graduate thesis, dissertation or practicum. A copy of the sponsoring college/university's approval letter and IRB letter must be attached to the application.

5.9.8. Approval of the Research Project Application by the Curriculum Staff Committee authorizes the applicant to proceed with the research/survey. Committee approval does not obligate the participation of any school or employee.

5.9.9. Following committee approval:

5.9.9.1. No changes in methodology or instrumentation may be made unless approved by the Curriculum Staff Committee.

5.9.9.2. A $100.00 refundable deposit is required. This deposit is to ensure that a copy of the research findings is shared with Nebo School District.

Once a copy of the research results are received by the Curriculum Coordinator, the $100.00 deposit will be refunded.

5.9.10. Upon completion of the research project, a copy of the research findings is to be submitted to the Curriculum Coordinator.

6. EXPUNGING DATA

6.1. Consistent with Utah law, this Plan "describes the [District's] expungement process, including how to respond to requests for expungement." UTAH CODE ANN. § 53E-9-301(7)(e) (2018). To expunge means to seal or permanently delete data.

6.2. In accordance with USBE rule, District records retention policies, and state retention schedules, the District requires expungement of student data.

6.3. Notwithstanding a request to expunge data, the District is prohibited from expunging grades, transcripts, a record of a student's enrollment, and assessment information.