

Morgan School District

Student Data Privacy and Security Governance Policy (pages 1-12) and IT Technology Security Plan (pages 13-20)

Statement of Purpose

The Morgan School District (“MSD”) affirms that the efficient collection, analysis, and storage of student information are essential to improve the education of our students. MSD recognizes the need to exercise care in the handling of confidential student information as the use of student data has increased and as technology has advanced. MSD also acknowledges that the privacy of students and the use of confidential student information is protected by federal and state laws, including the Family Educational Rights and Privacy Act (FERPA), the Utah Student Data Protection Act (“SDPA”), and the Utah Student Privacy Act (“SPA”). MSD acknowledges that violation of the Utah SDPA and SPA may result in civil penalties.

MSD’s *Student Data Privacy and Security Governance Policy* has been adopted in accordance with the SDPA, U.C.A. §§53A-1-1401 and the Utah SPA. The policy is designed to ensure only authorized disclosure of confidential information. The governance plan provides an organizational approach to the acquisition, use, security, and disposal of education data in order to protect student privacy. The Morgan Board of Education has designated the Superintendent, the Director of Technology, and individual school administrators as Student Data Privacy Managers.

Defined Terms

Administrative Security consists of policies, procedures, and personnel controls including security policies, training, audits, technical training, supervision, separation of duties, rotation of duties, recruiting and termination procedures, user access control, background checks, performance evaluations, disaster recovery, contingency, and emergency plans. These measures ensure that authorized users know and understand how to properly use the system in order to maintain security of data.

Aggregate Data is collected or reported at a group, cohort, or institutional level and does not contain Personally Identifiable Information (PII).

<https://ceds.ed.gov/domainEntitySchema.aspx>

Data Breach is the unauthorized acquisition of PII.

Logical Security consists of software safeguards for an organization's systems, including user identification and password access, authenticating, access rights, and authority levels. These measures ensure that only authorized users are able to perform actions or access information in a network or a workstation.

Personally Identifiable Information (PII) includes: a student's name; the name of the student's family; the student's address; the student's social security number; a student education unique identification number; or other indirect identifiers such as a student's date of birth, place of birth, or mother's maiden name; and other 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.

Physical Security describes security measures designed to deny unauthorized access to facilities or equipment.

Student Data means data collected at the student level and included in a student's educational records.

Unauthorized Data Disclosure is the intentional or unintentional release of PII to an unauthorized person or untrusted environment.

Collection

MSD follows applicable state and federal laws related to student privacy in the collection of student data.

Data Supervisory Officers

Superintendent or designee as LEA Data Manager

The Superintendent has the following data management responsibilities:

- To authorize and manage the sharing outside the school of PII from a cumulative record
- To share personally identifiable student data under the following circumstances:
 - Of a student with the student and the student's parent;
 - When required by State or Federal law;
 - In an aggregate form with appropriate data redaction techniques applied;
 - For a school official;
 - For an authorized caseworker or other representative of the Department of Human Services or the Juvenile Court;
 - In response to a subpoena issued by a court;
 - As directory information;

- In response to submitted data requests from external researchers or evaluators;
- To ensure that personally identifiable student data is not shared for the purpose of external research or evaluation.
- To create and maintain a list of all MSD staff has access to personally identifiable student data.
- To ensure annual MSD-level training on data privacy to all staff members, including volunteers.

Director of Educational Technology

The Director of Educational Technology has the following data management responsibilities:

- To act as the primary local point of contact for the state student data officer
- To act as the primary point of contact in supporting the Superintendent in administering oversight of student data
- To ensure compliance with security systems laws throughout the MSD system, including:
 - Providing training and support to applicable MSD employees, and,
 - Producing resource materials and plans for MSD data security
- To investigate complaints of alleged violations of systems breaches
- To provide an annual report to the Morgan Board of Education and the Morgan Technology Committee MSD's systems security needs.

Access to Personally Identifiable Information

- Unless prohibited by law or court order, MSD provides parents, legal guardians, or eligible students, as applicable, the ability to review their child's educational records and student performance data as per state and federal law;
- MSD allows for authorized purposes, uses, and disclosures of data maintained by MSD as a Local Education Agency (LEA);
- The Superintendent is responsible for granting, removing, and reviewing user access to student data.
- MSD allows parents, students, and the public access to information about student data privacy and the security safeguards that protect the data from unauthorized access and use;
- MSD provides contact information and a process for parents and students to request student and public school information from MSD consistent with the law;
- MSD's Audit Committee conducts an annual review of existing access and security safeguards;
- Access to PII maintained by MSD shall be restricted to: (1) the authorized staff of MSD who require access to perform their assigned duties; and (2) authorized employees of

the Utah State Board of Education who require access to perform their assigned duties; and (3) vendors who require access to perform their assigned duties.

- MSD's Student Data Privacy Manager may not share PII outside of the school as an educational entity without a data authorization except:
 - With the student and the student's parent;
 - With a school official;
 - With an authorized caseworker or other representative of the Department of Human Services or Utah Juvenile Court, Division of Juvenile Justice Services, Division of Child and Family Services, Division of Services for People with Disabilities;
 - In response to a subpoena issued by a court, but not outside of the use described in the subpoena; and
 - With a person to whom the Student Data Privacy Manager's education entity has outsourced a service or function to research the effectiveness of a program's implementation or to perform a function that the education entity's employees would typically perform.
- The Student Data Privacy Manager may not share PII for the purpose of external research or evaluation.

Security

- MSD has in place administrative security, physical security, and logical security controls to protect from a data breach or an unauthorized data disclosure.
- MSD shall immediately notify the State Superintendent of Public Instruction in the case of a confirmed data breach or a confirmed unauthorized data disclosure.
- MSD shall also notify in a timely manner affected individuals, students, and families if there is a confirmed data breach or a confirmed unauthorized data disclosure.
- If there is a release of a student's PII due to a security breach, MSD shall notify the student, if the student is an adult student. If the student is not an adult student, MSD will notify the student's parent or legal guardian.
- In accordance with R277-487-6, MSD acknowledges that data maintained by MSD, including data provided by contractors, may not be sold or used for marketing purposes (except with regard to authorized uses or directory information not obtained through a contract with an educational agency or institution).

Employee Non-Disclosure Assurances

All MSD employees, contractors, and volunteers must sign and obey the *MSD Employee and Volunteer Non-Disclosure Agreement* which describes the permissible uses of state technology and information.

Non-Compliance

Non-compliance with the *Non-Disclosure Agreement* shall result in consequences up to and including removal of access to MSD's network; if this access is required for employment, employees and contractors may be subject to dismissal.

Data Disclosure Protocols

This plan establishes the protocols and procedures for sharing data maintained by MSD consistent with the disclosure provisions of the Federal Family Educational Rights and Privacy Act (FERPA) and Utah's SDPA.

- MSD will provide parents with access to their child's educational records, or an eligible student access to his or her own educational records, within 45 days of receiving an official request.
- MSD is not required to and will not provide information to parents or an eligible student concerning another student, the financial records of parents, and confidential letters of recommendation if the student has waived the right to access.
- MSD is not required to provide data that it does not maintain, nor is MSD required to create education records in response to an eligible student's request.
- Publicly released reports shall not include PII and shall use aggregate data in such a manner that re-identification of individual students is not possible.
- MSD has clearly defined in its communication policy and in registration materials for parents what data is determined to be directory information.
- MSD notifies parents in writing at registration about directory information which includes PII and offers parents an opportunity to opt out of the directory. If a parent does not opt out, the release of the information as part of the directory is not a data breach or an unauthorized data disclosure.
- MSD provides a disclosure statement to parents or guardians of MSD students that meets the following criteria:
 - Is a prominent, stand-alone document;
 - Is annually updated and published on MSD's website;
 - States the necessary and optional student data that MSD collects;
 - States that MSD will not collect student data prohibited by the Utah Student Data Protection Act;
 - States that MSD will not share legally collectible data without authorization;
 - States that students and parents are responsible for the collection, use, or sharing of student data as described in Section 53A-1-1405 which states that a student owns his/her personally identifiable student data and that a student may

- download, export, transfer, save, or maintain the student’s data, including documents;
 - Describes how MSD may collect, use, and share student data;
 - Includes the following statements: “The collection, use, and sharing of student data has both benefits and risks. Parents and students should learn about these benefits and risks and make choices regarding student data accordingly.”
 - Describes in general terms how MSD stores and protects student data; and
 - States a student’s rights related to his/her data.
- MSD will train employees, aides, and volunteers regarding confidentiality of personally identifiable student information and student performance data, as defined in FERPA.

General Non-Disclosure Assurances

All student data used by MSD is protected as defined by FERPA and Utah statute. All MSD staff must sign a *MSD Employee and Volunteer Non-Disclosure Agreement* to verify acknowledgement, receipt, and intent to adhere to this *Data Governance Policy*.

All MSD employees will do the following:

- Complete student data privacy and security training;
- Consult with MSD internal data officers when creating or disseminating reports containing data;
- Use password-protected computers/devices when accessing any student-level or staff-level records;
- Refuse to share individual passwords for personal computers or data systems with anyone without authorized access;
- Log out of any data system/portal and close the browser after each use;
- Store sensitive data on appropriate, secured location;
- Keep printed reports with PII in a locked location while unattended;
- Use a secure document destruction service provided at MSD when disposing of such records;
- Refuse to share personally identifying data during public presentations, webinars, etc., if users need to demonstrate child/staff level data;
- Redact any PII information when sharing sample reports with general audiences in accordance with guidance provided by the student data manager;
- Take steps to avoid disclosure of PII in reports, such as aggregating, data suppression, rounding, recording, blurring, perturbation, etc.;
- Delete files containing sensitive data after using them on computers, or move them to secured servers or personal folders accessible only by authorized parties;

- NOT use email to send screenshots, text, or attachments that contain PII or other sensitive information. If users receive an email containing such information, they must delete the screenshots/text when forwarding or replying to these messages. If there is any doubt about the sensitivity of the data the Student Data Privacy manager should be consulted;
- Use secure methods when sharing or transmitting sensitive data as approved by MSD.
- Share within secured server folders appropriate for MSD's internal file transfer;
- NOT transmit child/staff-level data externally unless expressly authorized in writing by the data owner and then only transmit data via approved methods;
- Limit use of individual data to the purposes which have been authorized within the scope of job responsibilities.

Data Disclosure to Requesting External Person or Organizations

- MSD may not disclose personally identifiable information of students to external persons or organizations to conduct research or evaluation that is not directly related to a State or Federal program reporting requirements, audit, or evaluation.
- A requesting governmental agency must provide evidence of the Federal or State requirements to share data in order to satisfy FERPA disclosure exceptions. The Director of Educational Technology will ensure that the proper data disclosure avoidances are included if necessary.
- MSD may share data that do not disclose personally identifiable information with an external researcher or evaluator for projects unrelated to Federal or State requirements if the following conditions have been met:
 - A MSD Superintendent or administrator sponsors an external researcher or evaluator request;
 - Student data are not PII and are de-identified through disclosure avoidance techniques and other pertinent techniques as determined collaboratively by the Superintendent and the Director of Educational Technology.
 - Researchers and evaluators supply MSD a copy of any publication or presentation that uses MSD data at least 10 days prior to any publication or presentation.

Data Security and Privacy Training

- MSD will provide a range of training opportunities for all MSD staff, including volunteers, with authorized access to student educational data or confidential educator records in order to minimize the risk of human error and misuse of information.
- MSD will also require all employees and volunteers to sign both the *Employee Responsible Use Agreement*, which describes the permissible uses of technology and

information, and MSD's *Confidentiality Agreement*, which prohibits employees' disclosure of confidential personally identifiable information.

- MSD will also provide targeted security and privacy training for data stewards and IT staff, as well as for any other groups that collect, store, or disclose data.
- Participation in the training is required and documented.

Third Party Vendors

- MSD's contracts with outside vendors involving student data, which govern databases, online services, assessments, special education or instructional supports, shall include the following provisions which are intended to safeguard student privacy and the security of the data:
 - Requirement that the third party provider meet the definition of a school official under 34 CFR 99.31 (a)(1)(i)(B); this definition allows for the inclusion of professors, instructors, administrators, health staff, counselors, attorneys, clerical staff, trustees, members of committees and disciplinary boards, and a contractor, consultant, volunteer, or other party to whom the school has outsourced institutional services or functions.
 - Requirement that the third-party provider assure compliance with Utah's SDPA through its MOU with MSD;
 - Requirement that the contract between the LEA and the third party provider include a provision that the data is the property of MSD;
 - Requirement that the vendor agree to comply with any and all applicable state and federal law;
 - Requirement that the provider have in place administrative security, physical security, and logical security controls to protect from a data breach or unauthorized data disclosure;
 - Requirement that the provider restrict access to PII to the authorized staff or to only those providers who require such access to perform their assigned duties;
 - Prohibition against the provider's secondary use of PII including sales, marketing or advertising;
 - Requirement that MSD monitor and maintain control of the data;
 - Requirement that, if MSD contract with a third party provider to collect and have access to MSD's data as described in R277-487-3B(5), MSD must notify a student and the student's parent or guardian in writing that the student's data is collected and maintained by the third party provider;
 - Requirement for data destruction and an associated timeframe; and
 - Penalties for non-compliance with the above provisions.
- MSD's Third Party Contractors are legally allowed to engage in the following activities:

- The use of student data for adaptive learning or customized student learning purposes;
 - Marketing of an educational application or product to a parent or legal guardian of a student if the third party contractor did not use student data, shared by or collected on behalf of MSD, to market the educational application or product;
 - Use a recommendation engine to recommend services or content that relates to learning or employment within the third party contractor's internal application, if the recommendation is not motivated by payment or other consideration from another party;
 - Respond to a student's request for information or feedback, if the content of the response is not motivated by payment or other consideration from another party;
 - Use student data to allow or improve the operability and functionality of the third party contractor's internal application.
- At the completion of a contract with the MSD, if the contract has not been renewed, a third party contractor shall return all personally identifiable student data to MSD, and, to the maximum extent possible, delete all personally identifiable student data related to the third party contractor's work.
 - A third party contractor may not (except as provided in Subsection 6(b) of the Utah Student Data Protection Act):
 - Sell student data;
 - Collect, use, or share student data, if the collection, use, or sharing of the student data is inconsistent with the third party contractor's contract with MSD;
 - or
 - Use student data for targeted advertising.
 - A person may obtain student data through the purchase of, merger with, or otherwise acquiring of a third party contractor if the third party contractor remains in compliance with state and federal law, this policy, and MSD's previous contract with the original third party.
 - The provisions of this section of MSD's *Student Data Privacy and Security Policy* do not apply to the use of an external application, including the access of an external application with login credentials created by a third party contractor's internal application; nor do they apply to the providing of Internet service; nor do they impose a duty on a provider of an interactive computer service, as defined by the Utah SDPA.

Data Breach Protocols

MSD shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, MSD staff shall follow industry best practices in responding to the breach. Furthermore, MSD shall follow best practices for notifying affected parties, including students, in the case of an adult student, or parents or legal guardians, if the student is not an adult student.

- Concerns about security breaches must be reported immediately to the Superintendent, Director or Director of Educational Technology, or school administrator who will collaborate with appropriate MSD administrators to determine whether a security breach has occurred.
- If the MSD administrative team determines that one or more employees or contracted partners have substantially failed to comply with this policy and other relevant privacy policies, the team will determine appropriate consequences, which may include termination of employment or a contract and further legal action.
- Concerns about security breaches that involve the Director of Educational Technology must be reported directly to the Superintendent.
- Concerns about security breaches that involve the Superintendent must be reported directly to the President of the Morgan Board of Education.
- MSD will provide and periodically update, in keeping with industry best practices, resources for Utah LEAs in preparing for and responding to security breaches.

Record Retention and Expungement

MSD staff shall retain and dispose of student records in accordance with Section 63G-2-604, 53A-1-1407, and shall comply with active retention schedules for student records per the Utah Division of Archive and Record Services.

MSD recognizes the risk associated with data following a student year after year that could be used to mistreat the student. MSD shall review all requests for records expungement from parents and make a determination based on the following procedure.

7.1 Procedure

The following records may not be expunged: grades, transcripts, a record of the student's enrollment, assessment information.

The procedure for expungement shall match the record amendment procedure found in [34 CFR 99, Subpart C](#) of FERPA.

1. If a parent believes that a record is misleading, inaccurate, or in violation of the student's privacy, they may request that the record be expunged.
2. The LEA shall decide whether to expunge the data within a reasonable time after the request.
3. If the LEA decides not to expunge the record, they will inform the parent of their decision as well as the right to an appeal hearing.

4. The LEA shall hold the hearing within a reasonable time after receiving the request for a hearing.
5. The LEA shall provide the parent notice of the date, time, and place in advance of the hearing.
6. The hearing shall be conducted by any individual that does not have a direct interest in the outcome of the hearing.
7. The LEA shall give the parent a full and fair opportunity to present relevant evidence. At the parents' expense and choice, they may be represented by an individual of their choice, including an attorney.
8. The LEA shall make its decision in writing within a reasonable time following the hearing.
9. The decision must be based exclusively on evidence presented at the hearing and include a summary of the evidence and reasons for the decision.
10. If the decision is to expunge the record, the LEA will seal it or make it otherwise unavailable to other staff and educators.

Quality Assurances and Transparency Requirements

The quality of data is a function of accuracy, completeness, relevance, consistency, reliability, appropriate accessibility, and data interpretation and use. This policy is structured to encourage the effective and appropriate use of educational data. MSD acknowledges that

adherence to compliance and data-driven decision-making guide what data is collected, reported, and analyzed at the school.

- Where possible, data are collected at the lowest level available (at the student/teacher level); no aggregate data collections are necessary if the aggregate data can be derived or calculated from the detailed data;
- For all data collections, MSD establishes clear guidelines for data collection and the purpose of the data request;
- MSD's State-level data are audited by external, independent auditors yearly as a check on accuracy or to investigate the source of any anomalies;
- Before releasing high-risk data, the Superintendent and Director of Educational Technology must complete a review of the reliability, validity, and presentation of the data, and must follow all protocols in this policy related to appropriate disclosure.

Data Transparency

In accordance with the Utah SDPA, MSD will annually publish all its disclosures of student personally identifiable information on the Utah State [Metadata Dictionary](#) developed by USBE and located on the Data Gateway. MSD will also provide a link from its webpage to the Metadata Dictionary where this disclosure may be found.

Morgan School District

Technology Security Policy

The Morgan Board of Education of the Morgan School District (“MSD”) has established this policy in order to support the maintenance and protection of student data and other education-related data or information that MSD stores, transmits, or otherwise manages by technology.

This policy is part of MSD’s overall Data Governance Plan and follows the guidelines and requirements set forth in *Utah’s Student Data Protection Act (SDPA)*, U.C.A §53A-1-1401 *et seq.* The policy also supports MSD’s *Student Data Privacy and Security Governance Policy*. In addition, MSD conforms with all federal and state privacy and governance laws including the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 (hereinafter “FERPA”), the Government Records and Management Act U.C.A. §62G-2 (hereinafter “GRAMA”), U.C.A. §53A-1-1401 *et seq.* and Utah Administrative Code R277-487.

Purpose

The purpose of this policy is to identify the rules and procedures for all individuals accessing and using MSD’s Information Technology assets and resources and to ensure that all users abide by the prescriptions regarding the security of data stored digitally within the boundaries over which MSD has direct authority or contractual authority.

Technology Security

MSD supports a secure network systems, including security for all personally identifiable information that is stored on paper or stored digitally on MSD-maintained computers and networks. This policy supports efforts to mitigate threats that may cause harm to MSD, its students, or its employees.

- MSD will ensure reasonable efforts to maintain network security.
- MSD acknowledges that data loss can be caused by human error, hardware malfunction, natural disaster, security breach, etc. and may not be preventable.
- All persons granted access to MSD’s network and other technology resources are expected to be careful and aware of suspicious communications and unauthorized use of MSD devices and the network.
- When an employee or other user becomes aware of suspicious activity, he/she must immediately contact the Superintendent or Director of Educational Technology with the relevant information.

- MSD requires all third-party vendors/contractors that have access to critically sensitive data to sign a *Memorandum of Understanding between MSD and Third-Party Vendors* before these vendors/contractors have access to MSD's systems or information.

Sustainability

Professional development for staff and students regarding the importance of network security and best practices is included in this policy's procedures. The procedures associated with this policy are consistent with guidelines provided by cyber security professionals worldwide and in accordance with Utah Education Network and the Utah State Office of Education. MSD supports the development, implementation, and ongoing improvement that produce a robust security system of hardware and software designed to protect data, users, and electronic assets.

Definitions

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

Authorization: Having 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.

Computer: Any electronic device or communication facility that stores, retrieves, processes, or transmits data.

Computer System: A set of related, connected or unconnected, devices, software, or other related computer equipment.

Computer Network: 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.

Computer Property: Electronic impulses, electronically produced data, information, financial instruments, software, or programs, in either machine or human readable form, and any other tangible or intangible item relating to a computer, computer system, computer network, and copies of any of the above.

Confidential Information: Data, text, or computer property that is 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.

Encryption or Encrypted Data: The translation of data into another form or code so that only people with access to a decryption key or password can access the data.

Personally Identifiable Information: Any data that may potentially identify a specific individual or any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data.

Security System: A computer, computer system, network, or computer property that has some form of access control technology, such as encryption, password protection, other forced authentication, or access control designed to keep out unauthorized persons.

Sensitive Data: Data that contains personally identifiable information.

System Level: Access to the system that is considered full administrative access, including operating system access and hosted application access.

Security Responsibility: MSD has appointed the Superintendent and the Director of Educational Technology as IT Security Officers responsible for overseeing MSD-wide IT security, to include the development of MSD's policies and adherence to the standards defined in this policy and related policies.

Training

- MSD shall ensure that all MSD employees who have access to sensitive information receive annual IT security training that emphasize their personal responsibility for protecting student and employee information.
- MSD shall ensure that all students are informed of Cyber Security Awareness.

Physical Security

Computer Security

MSD shall ensure that any user's computer will not be left unattended and unlocked, especially when logged into sensitive systems or data, including student or employee information.

Automatic log off, locks and password screen savers will be used to enforce this requirement.

MSD shall also ensure that all equipment that contains sensitive information will be secured in order to deter theft.

Server/Network Room Security

MSD shall ensure that server rooms and telecommunication rooms/closets are protected by appropriate access control which segregates and restricts access from general school or office areas. Access control shall be enforced using either keys, electronic card readers, or a similar method so that only those IT or other staff members having access necessary to perform their job functions are allowed unescorted access.

Telecommunication rooms/closets may only remain unlocked or unsecured when because of building design it is impossible to do otherwise or due to environmental problems that require the door to be opened.

Contractor Access

Before any contractor is allowed access to any computer system, server room, or telecommunication room, the contractor will need to present a company issued identification card, and his/her access will need to be confirmed directly by the authorized employee who issued the service request or by MSD's Superintendent or Director of Educational Technology.

Network Security

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

Network Segmentation

MSD shall ensure that all untrusted and public access computer networks are separated from its main computer network and will utilize security policies to ensure the integrity of those computer networks. MSD will also utilize industry standards and current best practices to segment internal computer networks based on the data they contain. This action will be taken to prevent unauthorized users from accessing services unrelated to their job duties and to minimize potential damage from other compromised systems.

Wireless Networks

No wireless access point shall be installed on MSD's computer network that does not conform with current network standards as determined by the Director of Educational Technology. Any exceptions to this must be approved directly in writing by the Superintendent. MSD shall scan

for and remove or disable any rogue wireless devices on a regular basis. All wireless access networks shall conform to current best practices and shall utilize at minimal WPA encryption for any connections. Open access networks are not permitted, except on a temporary basis when deemed necessary.

Remote Access

MSD shall ensure that any remote access with connectivity to MSD's internal network is achieved using the MSD's centralized VPN service that is protected by multiple factor authentication systems. Any exception to this policy must be due to a service provider's technical requirements and must be approved by the Director of Educational Technology.

Access Control

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.

Authentication

MSD shall enforce strong password management for employees, students, and contractors.

- Password Creation: All server system-level passwords must conform to the password construction guidelines determined by the Director of Educational Technology as per the Data Governance Plan.
- Password Protection: Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
- 2-Step Verification is required for all MSD staff accounts.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords may not be revealed on questionnaires or security forms.
- The content or format of passwords may not be disclosed in an insecure communication or as a hint.
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

Authorization

MSD shall ensure that user access shall be limited to only those specific access requirements necessary for employees to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access. MSD shall ensure that user access will be granted

and/or terminated upon timely receipt, and the Administration's approval, of a documented access request/termination.

Accounting

MSD 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, and failed attempts to access objects by unauthorized users, etc.

Administrative Access Controls

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

Incident Management

MSD will design its monitoring and response to IT related incidents to provide early notification of events and rapid response and recovery from internal or external network or system attacks.

Business Continuity

To ensure continuous critical IT services, MSD will develop a business continuity/disaster recovery plan appropriate for the size and complexity of MSD IT operations. MSD shall also develop and deploy a district-wide business continuity plan which should include as a minimum:

- 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. As a minimum, backup media must be stored off-site a reasonably safe distance from the primary server room.
- Secondary Locations: Identify a backup processing location.
- 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 students.

Malicious Software

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

- MSD shall install, distribute, and maintain spyware and virus protection software on all district-owned equipment, i.e. servers, workstations, and laptops.
- MSD shall ensure that malicious software protection will include frequent update downloads (minimum weekly), frequent scanning (minimum weekly), and that malicious software protection is in active state (real time) on all operating servers/workstations.
- MSD shall ensure that all security-relevant software patches (workstations and servers) are applied within thirty days and critical patches shall be applied as soon as possible.
- MSD will ensure that all computers use MSD's approved anti-virus solution.
- Any exceptions this section must be approved by the Director of Educational Technology or Superintendent .

Internet Content Filtering

In accordance with Federal and State Law, MSD shall filter internet traffic for content defined in law that is deemed harmful to minors.

- MSD acknowledges that technology-based filters are not always effective at eliminating harmful content and, therefore, MSD uses a combination of technological means and supervisory means to protect students from harmful online content.
- MSD provides a technology based filtering solution for MSD devices that students in assigned grades take home.
- MSD personnel supervise students when they access the internet using MSD-owned devices on school property.
- MSD relies on parents to provide the physical supervision necessary to protect students from accessing harmful online content at home.

Data Privacy

MSD considers the protection of the data it collects on students, employees and their families to be of the utmost importance.

- MSD protects student data in compliance with the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 ("FERPA"), the Government Records and Management Act U.C.A. §62G-2 ("GRAMA"), U.C.A. §53A-1-1401 et seq., 15 U.S. Code §§ 6501–6506 ("COPPA"), and Utah Administrative Code R277-487 ("Student Data Protection Act").
- MSD shall ensure that access to employee records shall be limited to only those individuals who have specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

Security Audit and Remediation

MSD shall perform routine security and privacy audits in congruence with the MSD Data Governance Plan. MSD personnel shall develop remediation plans to address identified lapses in accordance with MSD Information Security Remediation Plan.

Employee Disciplinary Actions

Employee Disciplinary Actions shall be in accordance with applicable laws, regulations and MSD policies. Any employee found to be in violation of this policy or related policies may be subject to disciplinary action up to and including termination of employment with MSD.