Morgan School District
Student Data Privacy and Security Governance Policy

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 M*SD 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 M*SD 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.

- In accordance with 53A-1-1407, MSD shall expunge student data that is stored upon the request of a student, if the student is at least 23 years old.
- MSD may expunge medical records and behavioral test assessments.
- MSD will not expunge student records of grades, transcripts, or records of a student's enrollment or assessment information except as allowed by law.
- MSD will collaborate with Utah State Archives and Records Services in updating data retention schedules. Student-level discipline data will be expunged after three years.

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

Employee Non-Disclosure Agreement

As an employee of the Morgan School District, I hereby affirm that:

_____ I have read MSD's *Student Data Privacy and Security Governance Policies,* which includes *Employee Non-Disclosure Assurances*.

_____ I understand the policy and the non-disclosure assurance that address general procedures, data use/sharing, and data security.

_____ I will abide by the terms of the MSD's policies and their processes and procedures. related to student data privacy and security.

_____ I grant permission for the manual and electronic collection and retention of security-related information, including but not limited to photographic or videotape images, of attempts to access the facility and/or workstations.

Trainings

_____ I have completed MSD's Data Security and Privacy initial training.

_____ I will complete MSD's Data Security and Privacy initial training within 30 days.

MSD Data and Reporting Systems

_____ I will use a password-protected computer when accessing data and reporting systems, viewing child/staff records, and downloading reports.

_____ I will not share or exchange individual passwords, either for personal electronic device/s or MSD system user accounts, with MSD staff or participating program staff.

_____ I will log out of and close the browser after each use of MSD data and reporting systems.

_____ I will access only data in which I have received explicit written permission/s from the data owner.

_____ I will not attempt to identify individuals, except as is required to fulfill job or volunteer duties, nor will I publicly release confidential data.

Handling Sensitive Data

_____ I will keep sensitive data on password-protected, state-authorized electronic devices.

_____ I will keep any printed files containing personally identifiable information in a locked location while unattended.

_____ I will not share child/staff-identifying data during public presentations, webinars, etc. I understand that dummy records should be used for such presentations.

_____ After working with them, I will delete files containing sensitive data from my desktop or device, or move them to a secured MSD server.

Reporting and Data Sharing

_____ I will not re-disclose or share any confidential data analysis without MSD's expressed written consent, except to other authorized personnel.

_____ I will not publically publish any data without the approval of the Superintendent.

_____ I will take steps to avoid disclosure of personally identifiable information in State-level reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.

_____ I will not use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If I receive an email containing such information, I will delete the screenshots or text when forwarding or replying to these messages.

_____ I will not transmit child/staff-level data externally unless explicitly authorized in writing.

_____ I understand that, when sharing child/staff-identifying data with authorized individuals, the only approved methods are phone calls or MSD's secure file transfer protocol.

_____ I understand that sharing within secured server folders is appropriate for MSD's internal file transfer.

_____ I will immediately report any data breaches, suspected data breaches, or any other suspicious activity related to data access to my supervisor, the Director of Educational Technology, or the Superintendent.

_____ I acknowledge my role as a public servant and steward of child/staff information, and affirm that I will handle personal information with care in order to prevent disclosure.

Consequences for Non-Compliance

_____ I understand that access to the MSD network and systems can be suspended based on any violation of this agreement or risk of unauthorized disclosure of confidential information.

_____ I understand that failure to report a violation of confidentiality by others is just as serious as my own violation and may subject me to personnel action, including termination.

Discontinuation of Employment

_____ I agree that, upon the discontinuation of my employment at MSD, I will not disclose or otherwise disseminate any confidential or personally identifiable information to anyone outside of MSD without the prior written permission of the Superintendent or Director of Educational Technology.

Printed Name____

Signature____

Date__________________________________

MEMORANDUM OF UNDERSTANDING

This Memorandum of Understanding ("MOU") is entered into by and between ________________________ ("Contractor") and the Morgan School District ("MSD") for the purpose of accessing student information as necessary for the vendor's provision of services to MSD. The provision of specific services may require MSD to disclose personally identifiable information (PII) about students that is protected under the *Family Educational Rights and Privacy Act* ("FERPA") (20 U.S.C. §1232g; 34 CFR Part 99) and Utah's Government Records and Management Act ("GRAMA") (Utah Code Ann. §63G-2-101 et seq.).

DATA PRIVACY

The Contractor will use MSD's data only for the purpose of fulfilling its duties under this MOU and will not share such data with or disclose it to any third party without the prior written consent of MSD, except as provided for in this MOU or as otherwise required by law.

MSD's data will not be stored outside the United States without prior written consent from MSD.

The Contractor will provide access to MSD's data only to its employees and subcontractors who need to access the data to fulfill the Contractor's obligations under this MOU. The Contractor will ensure that employees who perform work under this MOU have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of this MOU.

The following provision applies only if the Contractor will have access to MSD's education records as defined under FERPA. The Contractor acknowledges that for the purposes of this MOU it will be designated as a "school official" with "legitimate educational interests" in MSD education records, as those terms have been defined under FERPA and its implementing regulations, and the Contractor agrees to abide by the limitations and requirements imposed on school officials under that act.

The Contractor will use the education records only for the purpose of fulfilling its duties under this MOU for the benefit of MSD and its End User, and will not share such data with or disclose it to any third party except as provided for in this MOU, required by law, or authorized in writing by MSD.

The Contractor understands that there is a strict prohibition against the Contractor's secondary use of PII including sales, marketing or advertising, that the Contractor may not sell student data, or collect, use, or share student data if the collection, use, or sharing of the student data is inconsistent with the Contractor's contract with MSD. The Contractor also acknowledges that MSD has the authority to monitor and maintain control of the data.

EXCEPTIONS

The provisions of this MOU between MSD and the Contractor 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 Student Data Protection Act.

The obligations of this MOU shall not apply to any information which (a) is already in the public domain through no breach of this MOU, including but not limited to information available through the school's website; (b) information that was lawfully in the Contractor’s possession prior to receipt from MSD, its faculty, staff, or students; or (c) is received by the Contractor independently from a person or entity free to disclose such information lawfully (not a school, its faculty, staff, or students).

DATA SECURITY

The Contractor will store and process MSD's data in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure the Contractor's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved. Without limiting the foregoing, the Contractor warrants that all electronic MSD data will be encrypted/secured in transmission (including via web interface) in accordance with the latest version of National Institute of Standards and Technology Special Publication 800-53.

If the Contractor stores PII as part of this MOU, the Contractor warrants that the information will be stored in accordance with the latest version of National Institute of Standards and Technology Special Publication 800-53. The Contractor will use industry-standard and up-to-date security tools and technologies, such as anti-virus protections and intrusion detection methods, in providing Services under this MOU.

SECURITY BREACH

Upon becoming aware of a security breach, or of circumstances that are reasonably understood to suggest a likely security breach, the Contractor will notify MSD in a time frame consistent with applicable state or federal laws, fully investigate the incident, and cooperate fully with MSD's investigation of and response to the incident. Except as otherwise required by law, the Contractor will not provide notice of the incident directly to individuals whose personally identifiable information was involved, regulatory agencies, or other entities, without prior written permission from MSD.

LIABILITY

If the Contractor must under this MOU create, obtain, transmit, use, maintain, process, or dispose of the subset of MSD's data known as personally identifiable information, the following provisions apply. In addition to any other remedies available to MSD under law or equity, the Contractor will reimburse MSD in full for all costs incurred by MSD in the investigation and remediation of any security breach caused by the Contractor, including but not limited to providing notification to individuals whose personally identifiable information was compromised and to regulatory agencies or other entities as required by law or contract; providing one year's credit monitoring to the affected individuals if the personally identifiable information exposed during the breach could be used to commit financial identity theft; and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the security breach.

If the Contractor will NOT under this MOU create, obtain, transmit, use, maintain, process, or dispose of the subset MSD's data known as personally identifiable information, the following provisions apply. In addition to any other remedies available to MSD under law or equity, the Contractor will reimburse MSD in full for all costs reasonably incurred by MSD in investigation and remediation of any security breach caused by the Contractor.

DATA TRANSFER UPON TERMINATION OR EXPIRATION

Upon termination or expiration of this MOU, the Contractor will ensure that all of MSD's data is securely returned or destroyed as directed by MSD in its sole discretion. Transfer to MSD or a third party designated by MSD shall occur within a reasonable period of time, and without significant interruption in service. The Contractor shall ensure that such transfer/migration uses facilities and methods that are compatible with the relevant systems of MSD or its transferee, and to the extent technologically feasible, so that MSD will have reasonable access to MSD's data during the transition.

In the event that MSD requests destruction of its MSD data, the Contractor agrees to destroy in a secure manner all data in its possession and in the possession of any subcontractors or agents to which the Contractor may have transferred MSD's data. The Contractor agrees to provide documentation of data destruction to MSD.

The above provisions will also apply if the Contractor ceases its business operations prior to the expiration or termination of this MOU. Accordingly, the Contractor must notify MSD of impending cessation of its business and any contingency plans.

TERMS AND TERMINATION

Either party may terminate this MOU, for cause or convenience, upon thirty (30) days' written notice to the other party.

This MOU will be effective for one year from the date of execution as indicated below except that the parties may agree to up to three (3) successive one-year extensions. If the parties choose to extend this MOU, the parties must annually agree in writing to the extension at least thirty (30) days prior to the termination of the then-current one-year period.

By signing this MOU, the Contractor warrants and represents that it shall, at all times, comply with the terms of this MOU and with FERPA and GRAMA, and further agrees not to disclose or re-disclose to any person or entity for any purpose whatsoever any personally identifiable student information, as that term is defined by this MOU, by FERPA, and by GRAMA.

The parties agree that the individuals signing this MOU have the authority to bind their respective entities, that this MOU represents the entire agreement of the parties, and that no other superseding or binding promises or conditions exist in any other agreement either oral or written related to the topics covered herein. The parties also stipulate that this Agreement may not be modified except by the written consent of MSD.

Company Name____

Signature: ____________________________________ Date: _________________

Print Name/Position: ____

For the Morgan School District

Signature: ____________________________________ Date: _________________

Print Name/Position: ____