

# Data Governance Plan

## 1. PURPOSE

Mountain Heights Academy (the “School”) takes seriously its moral and legal responsibility to protect student data privacy and ensure student data security. The School is required by Utah’s student data protection laws and the School’s Student Data Privacy and Security Policy to establish a Data Governance Plan. This administrative Data Governance Plan encompasses the full life cycle of the School’s student data, from acquisition, to use, to disposal.

## 2. SCOPE AND APPLICABILITY

This Plan is applicable to all employees, volunteers, and third-party contractors of the School. The School will use this Plan, along with all policies and procedures of the School concerning student data privacy and security, to manage and address student data issues, assess agreements that permit disclosure of student data to third parties, assess the risk of conducting business with such third parties, and help ensure that the School makes only authorized disclosures of personally identifiable student data to third parties.

This Plan contains the School’s data governance procedures and processes related to the following:

1. Roles and Responsibilities;
2. Data Collection;
3. Data Use;
4. Data Storage;
5. Data Sharing;
6. Record Retention and Expungement;
7. Data Breach;
8. Data Transparency;
9. Data Privacy and Security Auditing; and
10. Data Privacy and Security Training.

This Plan refers to and works in conjunction with the School’s Student Data Privacy and Security Policy, Family Educational Rights and Privacy Policy and Administrative Procedures (“FERPA Policy” and “FERPA Administrative Procedures”), Metadata Dictionary, and Student Data Collection Notice.

In addition, this Plan works in conjunction with the School’s Information Technology Security Policy and accompanying Information Technology Systems Security Plan. The Information Technology Systems Security Plan contains procedures and processes related to the following:

1. System Administration;
2. Network Security;
3. Application Security;

4. Endpoint, Server, and Device Security;
5. Identity, Authentication, and Access Management;
6. Data Protection and Cryptography;
7. Monitoring, Vulnerability, and Patch Management;
8. High Availability, Disaster Recovery, and Physical Protection;
9. Incident Responses;
10. Acquisition and Asset Management; and
11. Policy, Audit, and E-Discovery Training.

### **3. ROLES AND RESPONSIBILITIES**

All student data utilized by the School is protected pursuant to the Family Educational Rights and Privacy Act and its regulations (20 U.S.C. § 1232g, 34 CFR Part 99) (“FERPA”), the Protection of Pupil Rights Amendment and its regulations (20 U.S.C. § 1232h, 34 CFR Part 98) (“PPRA”), and Utah’s student privacy and data protection laws and related USBE rules (Utah Code, Title 53E, Chapter 9, Parts 1-3, R277-487). The School designates managers to fulfill certain responsibilities regarding student data privacy and security. The School also imposes responsibilities on School employees and volunteers. The roles and responsibilities listed below outline some of the ways School managers, employees, volunteers, and third-party contractors are to utilize and protect personally identifiable student data.

#### **3.1 Student Data Manager**

The School’s Director serves as the School’s Student Data Manager and is responsible for student data privacy and security, including the following:

1. Acting as the primary local point of contact for the state student data officer described in Utah Code § 53E-9-302;
2. Authorizing and managing the sharing, outside of the School, of personally identifiable student data for the School as described in Utah Code § 53E-9-308;
3. Ensuring that no personally identifiable student data is shared without written consent (as defined in Utah Code § 53E-9-301) unless such sharing is:
  - a. To the student or student’s parent or guardian;
  - b. In accordance with FERPA and PPRA;
  - c. As required by federal law; or
  - d. As described in Utah’s student data protection laws, including Utah Code § 53E-9-308;
4. Ensuring that no personally identifiable student data is shared for the purpose of external research or evaluation unless all the requirements listed in Utah Code § 53E-9-308 are satisfied and the School’s review process set forth in Section 7 of this Plan is followed;
5. Ensuring that all aggregate data shared outside of the School without written consent is shared in accordance with Utah Code § 53E-9-308 and the School’s review process set forth in Section 7 of this Plan;

6. Ensuring that a list of all School employees who have access to personally identifiable student data is created, maintained, and provided to the School's Board of Directors, in accordance with Utah Code § 53E-9-204;
7. Ensuring all School employees and volunteers who are authorized by the School to have access to education records (1) receive annual student data privacy training and (2) that employees sign a statement certifying that they have completed the training and understand student data privacy requirements. Document names of all those who are trained, as well as the training dates, times, locations, and agendas;
8. Ensuring that the School's Student Data Collection Notice is created, annually updated, published, and distributed to parents and students as required by law;
9. Ensuring that the School's metadata dictionary is created, maintained, published, and provided to the Utah State Board of Education ("USBE") as required by law; and
10. Ensuring that this Plan is maintained, published, and provided to the USBE as required by law.

### **3.2 IT Security Manager**

The School's contracted IT provider will function as the School's IT Security Manager. The IT Security Manager's responsibilities include the following:

1. Overseeing IT security at the School;
2. Helping the School to comply with IT security laws applicable to the School;
3. Providing training and support to School employees on IT security matters;
4. Investigating complaints of alleged violations of the School's IT security policies, procedures, or plans;
5. Investigating alleged security breaches of the School's IT systems; and
6. Reporting periodically to the School's Board of Directors on the security of the School's IT systems.

### **3.3 Employees and Volunteers with Access to Education Records**

Employees and volunteers of the School who have access to education records have responsibilities with respect to student data privacy and security, including:

1. Participating in student data privacy training each year as required by the School;
2. Signing a statement each year certifying completion of student data privacy training and understanding of student data privacy requirements as required by the School (not required of volunteers);
3. NOT sharing personally identifiable student data outside of the School unless authorized to do so by law and the Student Data Manager;

4. Using password-protected School-authorized computers when accessing the School's data systems or viewing or downloading any student-level records;
5. NOT sharing or exchanging individual passwords for School-authorized computers or School data systems with anyone;
6. Logging out of any School data system or portal and closing the browser after each use or extended absence;
7. Storing personally identifiable student data on appropriate, secured locations. Unsecured access and flash drives, DVD, CD-ROM or other removable media, or personally owned computers or devices, are not deemed appropriate for storage of personally identifiable student data unless authorized by the Student Data Manager;
8. Keeping printed documents with personally identifiable student data in a locked, secured location and using School-approved document destruction methods when disposing of such records;
9. NOT sharing personally identifiable student data during public presentations;
10. Using secure methods when sharing or transmitting personally identifiable student data with authorized individuals. Secure electronic methods include, but are not limited to, telephone calls, Movelt (when sending data to the State), and, where practical, encrypted email. Also, sharing within secured server folders is appropriate for School internal file transfer;
11. Taking steps to avoid disclosure of personally identifiable student data in authorized reports or materials available to the public, such as aggregating, data suppression, rounding, blurring, etc.;
12. Only accessing and using student data as authorized by the School to fulfil job or volunteer duties, and not for any other purpose;
13. Immediately reporting to the Student Data Manager any data breaches, suspected data breaches, or any other suspicious activity related to data access;
14. Consulting with the Student Data Manager regarding any questions about personally identifiable student data and related privacy laws, requirements, or concerns; and
15. Abiding by the requirements, processes, and procedures of this Plan.

### **3.4 Educators**

In addition to abiding by the employee responsibilities listed above, educators at the School are also responsible for the following:

1. NOT sharing personally identifiable student data through educational apps (or any other apps used for classroom instruction) unless and until the app has been approved as required by the Student Data Manager; and
2. Completing the student data security and privacy training for educators developed by the State Superintendent when required for the educator's re-licensure pursuant to R277-487.

### **3.5 Third-Party Contractors**

Third-party contractors who are not educational entities and have access to, collect, or receive personally identifiable student data pursuant to a contract with the School shall only use the data strictly for the purpose of providing the contracted product or service within the negotiated contract terms. Each third-party contractor is also responsible for:

1. Complying with the contract and entering into and complying with the School's Data Confidentiality Addendum or another approved data privacy agreement approved by the School;
2. Sharing, as authorized by law or a court order, student data as requested by law enforcement;
3. At the completion of a contract with the School (if the contract has not been renewed), returning or deleting upon request of the School all personally identifiable student data under the control of the School unless a student or the student's parent consents to the maintenance of the personally identifiable student data;
4. Not selling student data (except in connection with a purchase, merger, or acquisition of the third-party contractor as described in Utah Code § 53E-9-309);
5. Not collecting, using, or sharing student data if the collection, use, or sharing is inconsistent with the third-party's contractor's contract with the School; and
6. Not using student data for targeted advertising.

Third-party contractors are allowed to use student data and do other actions related to students and parents as set forth in Utah Code § 53E-9-309(4). Also, the provisions in Utah Code § 53E-9-309 do not apply to certain third-party contractors and providers as explained in Utah Code § 53E-9-309(7). In addition, provisions in Utah Code § 53E-9-309 relating to a student's student data does not apply to a third-party contractor if the School or third-party contractor obtains authorization from the following individual, in writing, to waive that provision: (1) the student's parent, if the student is not an adult student; or (2) the student, if the student is an adult student.

### **3.6 Consequences for Non-Compliance**

The responsibilities listed above are intended to minimize the risk of human error and the misuse of School students' personally identifiable student data. A person or entity's non-compliance with the roles and responsibilities listed above shall result in consequences for the person or entity up to and including removal of access to the School's network. If this access is required for employment or contracted services, employees and third-party contractors may be subject to dismissal.

## **4. DATA COLLECTION**

The School collects student data for two main purposes: to comply with state or federal law and to improve students' educational experience. Student data enables the School

to participate in state and federal education programs and to qualify for state and federal education funds. Student data also helps the School to better plan and personalize classroom instruction, increase student and teacher performance, and make informed decisions. The School collects student data primarily through parents or guardians completing the School's secure online lottery and registration packet, but it may also collect additional student data during the school year.

#### **4.1 Data Elements Collected by the School**

**4.1.1 Necessary Student Data.** The School collects student data defined as "necessary student data" in Utah Code § 53E-9-301(12). See the School's Student Data Collection Notice for a list of necessary student data that the School collects.

**4.1.2 Optional Student Data.** The School collects student data defined as "optional student data" in Utah Code § 53E-9-301(13). See the School's Student Data Collection Notice for a list of optional student data that the School collects.

**4.1.3 Personally Identifiable Student Data.** The School collects student data defined as "personally identifiable student data" in Utah Code § 53E-9-301(15), including:

1. A student's first and last name;
2. The first and last name of a student's family member (e.g., parent or guardian);
3. A student's or a student's family's (e.g., a parent or guardian's) home or physical address;
4. A student's email address or other online contact information;
5. A student's telephone number;
6. A student's health or disability data (health data collected includes vision and hearing impairment, medical conditions, medications taken during school hours, allergies, special dietary needs, and other); and
7. A student's education entity student identification number.

#### **4.2 Records Collected by the School**

In addition to the records collected by the School as explained above, the School collects the following records as required or allowed by Utah law:

1. A copy of a student's birth certificate;
2. A copy of a student's yellow immunization card from the state, other proof of immunizations, or an Immunization Exemption Waiver;
3. If applicable, a copy of a student's IEP, IHCP, or Section 504 Plan;
4. If applicable, copy of legal documents such as a divorce decree, custody order, restraining order, protective order, power of attorney, or guardianship letters or orders;
5. A copy of a transfer student's record from the student's previous school; and
6. Fee Waiver Application, as applicable

#### **4.3 Data Not Collected by the School**

The School does not collect a student's social security number or, except as required in Utah Code § 80-6-103, criminal record.

#### **4.4 Data Not Collected by the School Without Prior Written Consent**

The School follows Utah Code § 53E-9-203 by not collecting certain information from a student by way of a psychological or psychiatric examination, test, treatment, survey, analysis, or evaluation unless the School has received the prior written consent of the student's parent or legal guardian or an exception to the prior written consent rule applies. Please refer to the School's FERPA Administrative Procedures (particularly the "Activities Prohibited Without Prior Written Consent" Section) to see the types of information governed by Utah Code § 53E-9-203, the accompanying notice and consent requirements, and exceptions. These administrative procedures explain how the School complies with the statute.

### **5. DATA USE**

The School uses the student data it collects to conduct the regular activities of the School. School employees and volunteers shall only have access to student data for which they have a legitimate educational interest and shall not use student data for any improper or non-educational purpose. School employees and volunteers shall use student data only as authorized by the School to fulfill their respective job or volunteer duties. Please see the School's FERPA Administrative Procedures (particularly the "Student Education Records Management" Section) for a summary of School personnel who, generally, have a legitimate educational interest in having access to student data and the particular data to which they have access. To help protect the privacy and security of student data, School employees and volunteers who have access to student data will participate in student data privacy training each year as required by the School and employees will sign a statement certifying that they have completed the training and understand student data privacy requirements.

Student data use by outside parties shall be limited to those to whom the School has shared the data in accordance with the law and who have a legitimate need to use the data. For example, outside parties with whom the School has contracted to provide services or functions that the School's employees would typically perform may use student data for the purpose of providing the contracted product or service. Third-party contractors' use of student data shall be in accordance with their contract and Data Confidentiality Addendum or other approved data privacy agreement with the School, and in compliance with applicable law, including Utah Code § 53E-9-309 and administrative rules adopted by the USBE.

## **6. DATA STORAGE**

Please see the “Physical Protection” and “Technological Protection” Sections of the School’s FERPA Administrative Procedures to review the ways in which the School stores student data and protects stored data.

**6.1 Electronic Storage.** As explained in the School’s FERPA Administrative Procedures, most of the student data collected by the School (including the data collected through the School’s registration) is stored electronically by the School in Aspire, which is the student information system provided to Utah schools by the USBE. Aspire provides a secure location for the storage, maintenance, and transmission of student data. If the School chooses to use any additional student information systems, it will ensure that the system has adequate security protections. School employees and volunteers shall not store personally identifiable student data on their personal computers or devices, flash drives, or any other removable data storage media unless authorized by the Student Data Manager.

**6.2 Physical Storage.** Any printed documents containing personally identifiable student data is to be stored by the School in a secured, locked location, and access to such locations shall be determined by the Student Data Manager. School employees and volunteers shall not store documents with personally identifiable student data in physical locations away from the School, such as in their homes or vehicles, unless authorized by the Student Data Manager.

**6.3 Third-Party Contractors.** Third-party contractors shall store personally identifiable student data received from the School only in accordance with their contract and Data Confidentiality Addendum or other approved data privacy agreement with the School and applicable law.

## **7. DATA SHARING**

The School shall not share a student’s personally identifiable student data outside of the School unless the data is shared in accordance with FERPA the PPRA, Utah student privacy and data protection laws and related USBE rules, and any other applicable law. The School’s Student Data Manager authorizes and manages such data sharing and ensures compliance with applicable law.

### **7.1 Prior Written Consent**

Except as provided by law, the School shall not share a student’s personally identifiable data with anyone other than the student or the student’s parent or legal guardian unless the School first obtains prior consent from the student’s parent or guardian (or the student if the student is 18 years old or older). In order to be valid, the prior consent must:

1. Be in writing;

2. Be signed by the student's parent or guardian, or the student if he or she is 18 or older (electronic signatures are sufficient);
3. Specify the records or data to be disclosed;
4. State the purpose of the disclosure; and
5. Identify the party to whom the disclosure may be made.

As provided in the "Student Education Records Management" Section of the School's FERPA Administrative Procedures, a student's parent or guardian (or the student if the student is 18 years old or older) has the right to inspect and review all of the student's education records maintained by the School and the School must grant such requests within a reasonable period of time, not to exceed 45 days after the request has been received by the School. The School may impose requirements related to such requests, such that the request be in writing, signed, dated, and contain certain information. The School may also require proof of identity and relationship (parent or guardian) to the student before granting access to the student's records.

## **7.2. Exceptions to the Prior Consent Rule**

The School shall not share, outside of the School, a student's personally identifiable student data without obtaining prior written consent unless such sharing is:

1. To the student or student's parent or guardian;
2. In accordance with federal and Utah law, including FERPA, PPRA, and Utah's student data privacy and protection laws. Such authorized sharing includes:
  - a. To a school official who has a legitimate educational interest (a school official could be an employee or agent of the School that the School has authorized to request or receive student data on behalf of the School);
  - b. To a contractor, consultant, volunteer, or other party to whom the School has outsourced a service or function provided that the party (1) performs an institutional service or function for which the School would otherwise use employees; (2) is under the direct control of the School with respect to the use and maintenance of student data; and (3) is subject to the requirements of 34 CFR § 99.33(a) governing the use and redisclosure of personal identifiable information from education records;
  - c. To an authorized caseworker or other representative of the Department of Health and Human Services, but only as described in Utah Code § 53E-9-308(3);
  - d. To other schools that have requested the data and 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;
  - e. To appropriate parties in connection with an emergency if knowledge of the information is necessary to protect the health or safety of the student or other individuals;
  - f. To officials in the juvenile justice system as permitted by law;

- g. To the Comptroller General of the United States, the Attorney General of the United States, the Secretary of the U.S. Department of Education, or State and local educational authorities in connection with an audit or evaluation of federally or state supported education programs, or for the enforcement of, or compliance with, federal legal requirements relating to those programs;
- h. To the applicable entities/agencies within the Department of Homeland Security for foreign students attending the School under a visa;
- i. To the Attorney General of the United States in response to an *ex parte* order in connection with the investigation or prosecution of terrorism crimes;
- j. In response to a valid subpoena or court order; or
- k. The sharing of personally identifiable student data that is directory information, but only if the School (1) has given the student's parent annual notice of the types of data it has designated as directory information and of the parent's right to request that any or all of student's directory information not be released by the School; and (2) the parent has not notified the School that he or she does not want the student's directory information to be released.

### **7.3 Directory Information**

The School designates the following student data as directory information:

- 1. Name;
- 2. Photograph or video of the student; and
- 3. Grade Level.

The student data designated as directory information may change from time to time. Parents will be given notice of such changes as required by law.

### **7.4 Third-Party Contractor Addendum**

The School may share personally identifiable student data with third-party contractors pursuant to subsections (a) and (b) immediately above if the contractors have entered into a contract and Data Confidentiality Addendum (or other approved data privacy agreement) with the School. Third-party contractors must comply with the contract, Addendum/approved data privacy agreement, and Utah student data protection laws, including Utah Code § 53E-9-309, and related administrative rules adopted by the USBE.

### **7.5 Aggregate Data**

**7.5.1 Definition.** “Aggregate data” has the same meaning as set forth in Utah Code § 53E-9-301(2). Aggregate data does not reveal any personally identifiable student data and contains data of at least 10 individuals.

**7.5.2 Sharing Aggregate Data.** The School may share aggregate data outside of the School without obtaining prior written consent so long as it is shared in accordance with Utah Code § 53E-9-308 and this paragraph. If the School receives a request for aggregate data, including for the purpose of external research or evaluation, the School shall follow the review process set forth below:

1. All requests shall be submitted in writing to the Student Data Manager;
2. The written request to the Student Data Manager shall describe the purpose of the request, the desired student data, how the student data will be used, and details about how the student data will be disclosed or published by the requestor;
3. The Student Data Manager shall review the written request and consult with the School’s management company about any potential data privacy issues relevant to the request;
4. If the Student Data Manager approves of the request, an MOU shall be prepared and presented (along with the requestor’s written request) to the School’s Board of Directors for review and approval; if the Student Data Manager disapproves of the request, the requestor shall be so notified;
5. If the Board approves of the request and MOU, the MOU shall be signed by the Board’s president or designee, as applicable, and the requestor; if the Board disapproves of the request, the requestor shall be so notified;
6. After approval by the Board and execution of the MOU, the Student Data Manager or a responsible person designated by the Student Data Manager, shall, as applicable, de-identify the requested student data through disclosure avoidance techniques (such as data suppression, rounding, recoding, blurring, perturbation, etc.) and/or other pertinent techniques;
7. After all requested student data has been de-identified and reviewed by the Student Data Manager, the requested student data shall be saved, physically or electronically, in a secure location managed by the Student Data Manager and then sent to the requestor through a secure method approved by the Student Data Manager.

The School may not share personally identifiable student data with external persons or organizations to conduct research or evaluations unless such research or evaluations are directly related to a state or federal program audit or evaluation.

## **8. RECORD RETENTION AND EXPUNGEMENT**

Record retention and expungement procedures promote efficient management of records, preservation of records of enduring value, quality access to public information, and data privacy.

**8.1 Retention.** The School shall retain and dispose of student records in accordance with Utah Code § 63G-2-604, Utah Code § 53E-9-306, rules adopted by the USBE, including R277-487-4. Unless the School adopts its own approved retention schedule, the School shall comply with the model retention schedule for student records published by the Utah Division of Archives and Records Service, which is currently the Utah RAMP Utah Education Records Retention Schedule.

**8.2 Expungement.** The School shall comply with Utah Code § 53E-9-306 and R277-487-4 in terms of what student data it may and may not expunge. Accordingly, the School may not expunge a student's grades, transcripts, record of enrollment, or assessment information. The School may, on its own volition or at the request of a student's parent or an adult student, expunge other student data, including a student's medical records and behavioral assessments, so long as the administrative need for the student data has passed. A request to expunge such student data shall be made in writing to the School's Student Data Manager and describe in detail the data requested to be expunged.

In addition, a student's parent or an adult student may also request that the School expunge any student data or record not subject to a retention schedule under Utah Code § 63G-2-604, and believed to be

1. Inaccurate;
2. Misleading; or
3. In violation of the privacy rights of the student.

Such a request to expunge a student's student data or records shall be made in writing to the School's Student Data Manager and describe in detail the data or records requested to be expunged. The School will process such requests following the same procedures outlined for a request to amend a student record in 34 CFR Part 99, Subpart C. These procedures are outlined below:

1. If a parent or adult student 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 School shall decide whether to expunge the data within a reasonable time after the request.
3. If the School decides not to expunge the record, the School will inform the parent or adult student of its decision as well as the right to an appeal hearing.
4. The School shall hold a hearing within a reasonable time after receiving the request for a hearing.
5. The School shall provide the parent or adult student 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 School shall give the parent or adult student 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 School 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 School will seal it or make it otherwise unavailable to other School staff and educators.

The School may consult with the Utah Division of Archives and Records Service and/or USBE when issues or questions arise with respect to record retention and expungement.

**8.3 Disciplinary Record.** The School may create and maintain a disciplinary record for a student in accordance with rules adopted by the USBE.

## **9. DATA BREACH**

**9.1 Definition of Data Breach.** A data breach for purposes of this Plan is any instance in which there is an unauthorized release or access of personally identifiable student data. This definition applies regardless of whether the School stores and manages the data directly or through a third-party contractor.

**9.2 Types of Data Breaches.** Data breaches can take many forms, including:

1. Hackers gaining access to personally identifiable student data through a malicious attack (such as phishing, virus, bait and switch, keylogger, denial of service, etc.);
2. A School employee losing School equipment on which personally identifiable student data is stored (such as a laptop, thumb drive, cell phone, etc.) or having such equipment stolen;
3. An unauthorized third party retrieving personally identifiable student data from a School's physical files;
4. A School employee accidentally emailing personally identifiable student data to an unauthorized third party; or
5. A School employee or third-party contractor saving files containing personally identifiable student data in a web folder that is publicly accessible online.

**9.3 Industry Best Practices.** The School takes a variety of measures to protect personally identifiable student data, including imposing disclosure prevention responsibilities on School employees, educators, volunteers, and third-party contractors. The School also follows industry best practices to maintain and protect personally identifiable student data and to prevent data breaches, some of which are outlined in the School's Information Technology Systems Security Plan.

**9.4 Responding to a Data Breach.**

**9.4.1 Reporting a data breach.** School employees, volunteers, and third-party contractors shall immediately report a data breach or a suspected data breach to the Student Data Manager. Students and parents of students who become aware of a data breach or that suspect a data breach shall also immediately notify the Student Data Manager.

**9.4.2 Data Breach Protocol.** The Student Data Manager shall collaborate with the IT Security Manager and others, as appropriate, to determine whether a data breach has occurred. If it is determined that a data breach has occurred, the School shall, under the direction of the Student Data Manager and IT Security Manager, follow the protocol described below:

1. Lock down systems and data that have been breached or suspected to have been breached, including changing applicable passwords, encryption keys, locks, etc.;
2. Assemble a Data Breach Response Team, which could include the Student Data Manager, IT Security Manager, School employees, Board members, members of the School's management company, the School's IT provider, etc.;
3. Record as many details about the data breach as possible, including:
  - a. Date and time data breach was discovered;
  - b. Data elements involved (for example, students' first and last name, SSIDs, DOBs, passwords, account information, employee social security numbers, etc);
  - c. Data systems involved (for example, Aspire or other School data system); and
  - d. Type of data breach (physical, such as stolen/lost paperwork or computer equipment; or electronic, such as hacking or unauthorized email transmission).
4. Assign an incident manager that has the appropriate qualifications and skills to be responsible for the investigation of the data breach;
  - a. Investigate scope of data breach to determine types of information compromised and number of affected individuals; and
  - b. Investigate the data breach in a way that will ensure that the investigative evidence is appropriately handled and preserved;
5. Attempt to retrieve lost, stolen, or otherwise compromised data;
6. Determine whether notification of affected individuals is appropriate and, if so, when and how to provide such notification; notification timeframes and requirements should be identified as soon as possible and notices developed and delivered to affected individuals and agencies in accordance with regulatory mandates and timeframes;
7. If the data breach involved the release of a student's personally identifiable student data, notify the student (if the student is an adult student) or the student's parent or legal guardian if the student is not an adult student in a manner reasonable under the circumstances;
8. If the data breach constitutes a "significant data breach" as defined in R277-487, notify:

- a. The student (if the student is an adult student) or the student's parent or legal guardian if the student is not an adult student; and
  - b. The USBE within ten business days of the initial discovery of the significant data breach as required in R277-487-3;
9. Determine whether to notify the authorities/law enforcement (situation dependent); involve legal counsel to analyze legal obligations;
  10. If the School has cyber liability and/or data breach insurance coverage, determine whether to notify the insurance provider and make a claim on such coverage; and
  11. Consult with appropriate security professionals, as necessary, to identify the possible reason(s) for the data breach and how to prevent similar data breaches in the future.

Following the steps above and clearly defining the roles and responsibilities of all those involved in the steps will promote better response coordination and help the School shorten its incident response time. Prompt response is essential for minimizing the risk of any further data loss and, therefore, plays an important role in mitigating any negative consequences of the breach, including potential harm to affected individuals. All work and activities performed under each of the steps above should be well documented and all documentation should be retained as required.

#### **9.4.3 Coordination with Management Company and/or Legal Counsel**

The School shall coordinate with its management company and/or separate legal counsel on the preparation and method of delivery of written materials, including notifications, related to a data breach.

#### **9.5 Cooperation**

The School shall cooperate with regulatory and governmental agencies that make inquiries regarding a data breach.

### **10. DATA TRANSPARENCY**

The School's policies concerning data privacy and security are published on the School's website. In addition, each year the School shall publish its current version of the following on its website:

1. Metadata Dictionary;
2. Student Data Collection Notice;
3. Information Technology Systems Security Plan; and
4. Data Governance Plan.

### **11. DATA PRIVACY AND SECURITY AUDITING**

The School shall periodically conduct audits to determine compliance with this Plan and to assess the quality and effectiveness of the data privacy and security processes and

procedures set forth in this Plan. The School shall use the results of such audits to determine ways in which this Plan and the School's student data governance and management can be improved. The School may use third-party experts to assist with and/or conduct such audits.

The School or its designee may audit its third-party contractors to verify compliance with the terms of the School's Data Confidentiality Addendum or other data privacy agreement approved by the School that relate to the confidentiality and protection of personally identifiable student data.

## **12. DATA PRIVACY AND SECURITY TRAINING**

On an annual basis, the School shall provide appropriate student data privacy training to its employees, aides, and volunteers who are authorized by the School to have access to education records as defined in FERPA.

The School shall also provide its employees with appropriate training on IT security matters.

Where required by R277-487, educators at the School shall complete the student data security and privacy training for educators developed by the State Superintendent as a condition of re-licensure.