Mountain Heights Academy
LEADERS IN DIGITAL EDUCATION

# Administrative Procedures Manual

# Table of Contents


Attendance Policy Procedures ..... 1

Child Abuse and Neglect Reporting Policy Reporting Form ..... 3

Computer Requirements ..... 5

Data Governance Plan ..... 7

Donation of Paid Time Off Procedure ..... 26

Information Technology Systems Security Plan ..... 28

Laptop Use Agreement and Acceptable Use Policy for Students ..... 35

Public Education Engagement and Exit Survey Procedures ..... 42

Religion and Education Policy Procedures for Implementation ..... 45

Student Education Plan Procedures ..... 50

Time and Effort Documentation Procedures ..... 52

# Attendance Policy Procedures

**Mountain Heights Academy**
**Amended: August 30, 2024**

1. Records are maintained on a student information system.

2. Teachers and MHA administrators review attendance on a regular basis to determine that full-time students are on track to complete the 990 hours of instruction each year. Teachers will consistently contact the parent and/or student.

3. The applicable language and definitions in Utah Code § 53G-9-804(1)(a) and Utah Code §§ 53G-6-201 through 53G-6-211 apply with respect to the enforcement of MHA's Attendance Policy and Procedures.

4. MHA may issue notices of truancy to school-age children who are truant at least 5 times during the school year. A notice of truancy will only be issued after MHA has made earnest and persistent efforts to resolve student attendance problems. A notice of truancy will:
    a. Direct the student who receives the notice of truancy, and the parent of the student, to meet with designated MHA authorities to discuss the student's attendance problems and cooperate with MHA administration to secure regular attendance by the student; and
    b. Be served on the student's parent by personal service or regular mail.

5. In accordance with Utah Code § 53G-8-211, the School shall refer a student who is a habitual truant to an evidence-based alternative intervention described in Utah Code § 53G-8-211(3). If the student who is a habitual truant refuses to participate in an evidence-based alternative intervention, the School shall refer the student for prevention and early intervention youth services, as described in Section 80-5-201, by the Division of Juvenile Justice and Youth Services. The School may only refer a student who is a habitual truant to a law enforcement officer or agency or a court if:
    a. The student was previously alleged of being a habitual truant at least twice during the same school year; and

b. The student was referred to an evidence-based alternative intervention, or for prevention and early intervention youth services, as described above for at least two of the previous habitual truancies.

6. MHA will establish chronic absenteeism prevention and intervention measures to encourage good attendance, improve academic outcomes, and reduce negative behaviors. Through these measures, MHA hopes to create a trusting relationship between teachers, students, and parents.
    a. MHA's efforts to prevent chronic absenteeism include, but are not limited to:
        i. [insert prevention measure/effort];
        ii. [insert prevention measure/effort]; and
        iii. [insert prevention measure/effort].
    b. MHA will seek to help students struggling with absenteeism (including chronically absent students) through implementing research or evidence-based absenteeism and dropout prevention interventions. These interventions include, but are not limited to::
        i. [insert intervention];
        ii. [insert intervention]; and
        iii. [insert intervention].

7. Parents/guardians who believe that all or part of their student's unexcused absences or tardies should be considered excused, or if they want to contest a notice of truancy, habitual truancy referral, or any disciplinary action taken against their student pursuant to MHA's Attendance Policy or Procedures, shall follow MHA's Parent Grievance Policy.

8. If students with disabilities under the Individuals with Disabilities Education Act, or students protected under either Section 504 of the Rehabilitation Act or the Americans with Disabilities Act, have excessive absences, including but not limited to absences for mental or behavioral health reasons, and fall within the criteria of these Procedures, MHA will ensure that these Procedures are applied in a manner consistent with all applicable state and federal laws and regulations. Excused absences for known mental or behavioral health reasons do not absolve MHA of FAPE responsibilities.

9. MHA shall annually report the following data separately to the Utah State Board of Education:
    a. Absences with a valid excuse; and
    b. Absences without a valid excuse.

**Commented [A1]:** Examples: careful monitoring of absences, educating students and parents on school's attendance policies and procedures and expectations, providing incentives or rewards for good attendance, contacting parents after a student reaches 4 unexcused absences, issuing notices of truancy after 5 unexcused absences, etc.

**Commented [A2]:** Examples of interventions from Utah Code 53G-6-206 include mentorship programs, counseling, family connection to community resources, academic support thru small groups or individualized tutoring or similar methods, teaching executive function skills (planning, goal setting, understanding and following multi-step directions, and self regulation), issuing notices of truancy, making adustments to student's schedule or curriculum, participating in truancy mediations, meetings with student, parents, and teacher, etc.

# Child Abuse and Neglect Reporting Policy Reporting Form

Mountain Heights Academy
Adopted: October 5, 2015
Amended: October 5, 2018

***CONFIDENTIAL***

**Child Abuse and Neglect Reporting Form**

| ORAL REPORT MADE TO PRINCIPAL: | |
|---|---|
| **Date:** | **Time:** |

| CHILD'S INFORMATION: | | | |
|---|---|---|---|
| **Name:** | **Age:** | **Sex:** | **Birth Date:** |
| **Address:** | | | |

| PARENT/GUARDIAN INFORMATION: | |
|---|---|
| **Father Name:** | **Mother Name:** |
| **Father Address:** | **Mother Address:** |
| **Father Phone:** | **Mother Phone:** |
| | |
| **Guardian #1 Name:** | **Guardian #2 Name:** |
| **Guardian #1 Address:** | **Guardian #2 Address:** |
| **Guardian #1 Phone:** | **Guardian #2 Phone:** |

| CIRCUMSTANCES LEADING TO THE SUSPICION THAT THE CHILD IS A VICTIM OF ABUSE OR NEGLECT: |
|---|
| |
| |
| |

| DATE AND TIME OF OBSERVATIONS | |
|---|---|
| **Date:** | **Time:** |

| ADDITIONAL INFORMATION: |
|---|
| |
| |

| Oral Report Made To: | Written Report Made To: |
|---|---|
| **Agency:** | **Agency:** |
| **Individual's Name:** | **Individual's Name:** |
| **Date:** | **Date:** |
| **Time:** | **Time:** |

| Reporting Individual: | | Principal: | |
|---|---|---|---|
| Name: | | Name: | |
| Date: | | Date: | |
| Signature | | Signature: | |

*****DO NOT PLACE THIS FORM IN THE STUDENT'S CUM FILE*****

# Computer Requirements

**Mountain Heights Academy**
**Adopted:**

Students may provide and use their own equipment and software as long as they meet the minimum requirements detailed in this section. Mountain Heights Academy has no responsibility for providing any support for equipment or software that is not provided by Mountain Heights Academy.

Computer Requirements

- Windows 7, 8, 10 or Mac OS X 10.5 or later
- Minimum of 10 gigabytes free HDD space
- Broadband internet connection
- Minimum 1GB RAM (2 or more GB RAM Recommended)
- Webcam
- Audio: Sound card with speakers, microphone (or headset)
- Chrome Browser and Firefox Browser (PC), Safari and Chrome (Mac)

Downloads

- Chrome http://www.google.com/chrome/
- Firefox: https://www.mozilla.org/en-US/firefox/desktop/
- Cute PDF Writer http://www.cutepdf.com/
- Geogebra http://www.geogebra.org/cms/en/download
- Adobe Acrobat Reader http://get.adobe.com/reader/
- Flash Player http://get.adobe.com/flashplayer/
- Quicktime https://support.apple.com/en_US/downloads/quicktime
- Audacity http://audacity.sourceforge.net/download/
- Audacity LAME mp3 Encoder (required for saving audio files as mp3 http://lame.buanzo.org/#lamewindl

Recommended Chrome Browser Add-Ons

- Awesome Screenshot Capture and Annotate: https://chrome.google.com/webstore/detail/awesome-screenshot-screen/nlipoenfbbikpbjkfpfillcgkoblgpmj

# Data Governance Plan

Mountain Heights Academy
Data Governance Plan
Adopted: August 9, 2017
Revised: January 30, 2020

## 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 Act 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 Disclosure Statement.

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 federal Family Educational Rights and Privacy Act ("FERPA"), the Utah Family Educational Rights and Privacy Act ("Utah FERPA"), and the Utah Student Data Protection Act. 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 Ann. § 53A-1-1403;
2. Authorizing and managing the sharing, outside of the School, of personally identifiable student data from a cumulative record for the School, including

a. Ensuring that no personally identifiable student data is shared outside of the School without a data authorization unless such sharing is:
    i. To the student or student's parent or guardian; or
    ii. To other outside parties only as authorized by FERPA, Utah FERPA, and the Student Data Protection Act, including Utah Code Ann. § 53A-1-1409.
b. Ensuring that no personally identifiable student data is shared outside of the School for the purpose of external research or evaluation, unless required to do so by law.

3. Ensuring that all aggregate data shared outside of the School without a data authorization is shared in accordance with Utah Code Ann. § 53-1-1409(8)-(9) and the School's review process set forth in Section 7 of this Plan;
4. Creating and maintaining a list of all School employees who have access to personally identifiable student data and provide the list to the School's Board of Directors, in accordance with Utah Code Ann. § 53A-13-303;
5. 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) 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.
6. Ensuring that the School's student data disclosure statement is created, annually updated, published, and distributed to parents and students as required by law.
7. 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
8. 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. Sign 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, ownCloud, MoveIt (when sending data to the State), and 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 R277-487-13.

### 3.5 Third-Party Contractors

Third-party contractors who have access to or receive personally identifiable student data pursuant to a contract with the School shall only use the data for the purpose of providing the contracted product or service within the negotiated contract terms. Each third-party contractor is responsible for complying with the contract and entering into and complying with the Data Confidentiality Addendum approved by the School's Board of Directors.

### 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 a secure online 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 Ann. § 53A-1-1402(17), including:

1. Name (first, middle, and last);
2. Date of birth;
3. Gender;
4. Parent contact information (including full name, relationship to student, home address, phone number(s), and email address);
5. Custodial parent information (including contact information, whether living with student, and existence of any legal documents regarding custody of student);
6. Contact information (including phone number and home/mailing address);
7. A student identification number;
8. Local, state, and national assessment results or an exception from taking a local, state, or national assessment;
9. Courses taken and completed, credits earned, and other transcript information;
10. Course grades and grade point average;
11. Grade level and expected graduation date or graduation cohort;
12. Degree, diploma, credential attainment, and other school exit information;
13. Attendance and mobility;
14. Drop-out data;
15. Immunization record or an exception from an immunization record;
16. Race;
17. Ethnicity;
18. Tribal affiliation;
19. Remediation efforts;
20. An exception from a vision screening required under Utah Code Ann. § 53A-11-203 or information collected from a vision screening required under Utah Code Ann. § 53A-11-203;
21. Student injury information;
22. A cumulative disciplinary record created and maintained as described in Utah Code Ann. § 53A-1-1407;
23. Juvenile delinquency records;
24. English language learner status (including whether child speaks a language other than English);
25. Child find and special education evaluation data related to initiation of an IEP; and
26. Information related to School's Fee Waiver Application, including household income verification, whether student receives SSI benefits, whether family receives TANF, and whether student is in foster care or in

state custody.

**4.1.2 Optional Student Data.** The School collects the following student data defined as "optional student data" in Utah Code Ann. § 53A-1-1402(18):

1. Information that is not "necessary student data" described above but is related to a student's IEP or required for a student to participate in a federal or other program;
2. A student's preferred first, middle, and last name (but only if different than student's legal names);
3. A student's homelessness status;
4. Whether a student was born outside of the United States;
5. A student's disciplinary history, including whether a student has ever been suspended or expelled from school and if the student has any disciplinary action pending from the student's previous school of enrollment;
6. A student's emergency contact information (including name, relationship to student, and phone number(s)); and
7. Information need for School to facilitate transfer of a student's student records from previous school, including:
    a. Whether student currently resides in Utah;
    b. District boundaries in which student lives;
    c. School boundaries in which student lives;
    d. Whether student has pre-registered with a school other than the school located in the school boundaries in which student lives;
    e. Name and contact information (address and phone number) of the school in which the student has pre-registered.

**4.1.3 Personally Identifiable Student Data.** The School collects student data defined as "personally identifiable student data" in Utah Code Ann. § 53A-1-1402(20), including:

1. A student's first and last name;
2. The first and last name of a student's family member (parent or guardian);
3. A student's or a student's family's (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 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 Ann. § 78A-6-112, criminal record.

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

The School follows Utah Code Ann. § 53A-13-302 in Utah FERPA 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 Ann. § 53A-13-302, 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 "Access to Information" 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 with the School, and in compliance with applicable law, including Utah Code Ann. § 53A-1-1410 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 online registration system) 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 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, Utah FERPA, the Utah Student Data Protection Act, 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. 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. Authorized by federal and Utah law, including FERPA, Utah FERPA, and the Utah Student Data Protection Act. 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 person or entity to whom the School has outsourced a service or function (1) to research the effectiveness of a program's implementation or (2) that the School's employees would typically perform;
    c. To an authorized caseworker or other representative of the Department of Human Services, but only as described in Utah Code Ann. § 53A-1-1409(6);
    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 individuals who need to know in cases of health and safety emergencies;
    f. To officials in the juvenile justice system when the disclosure concerns the system's ability to effectively serve, prior to adjudication, the student whose data is to be released;
    g. 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 Immigration and Naturalization Service (INS) 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
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 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 personally identifiable student data to be designated as directory information.

**7.3 Directory Information**

The School designates the following student data as directory information:

1. Student's name;
2. Photograph or video of the student;
3. Grade level; and
4. City where student resides.

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 with the School. Third-party contractors must comply with the contract, Addendum, and the Utah Student Data Protection Act, including Utah Code Ann. § 53A-1-1410 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 Ann. § 53-1-1402(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 Ann. § 53-1-1409(8)-(9) 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 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 Ann. § 63G-2-604, Utah Code Ann. § 53E-9-306, and 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 schedules for student records published by the Utah Division of Archives and Records Service.

**8.2 Expungement.** The School shall comply with Utah Code Ann. § 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 Director 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 Ann. § 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 Director 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, online registration system, 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 involved the release of a student's personally identifiable student data by a third-party contractor of the School, notify the State Superintendent 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 Disclosure Statement;
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 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 R277-487-13, 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.

# Donation of Paid Time Off Procedure

**Mountain Heights Academy**
**Donation of Paid Time Off Procedure**
**Adopted: May 20, 2016**

**Purpose**

The purpose of this administrative procedure is to provide a mechanism by which employees of Mountain Heights Academy (the "School") can voluntarily donate paid time off ("PTO") days to other staff members under extraordinary circumstances.

**Procedure**

1. An employee, or an employee's immediate family member, must be experiencing a catastrophic illness in order to be eligible to receive donated leave. Catastrophic illness includes but is not limited to a life threatening illness that requires the employee to be absent from work for an intermittent and/or extended period of time or a medical emergency that results in absence from work for at least one week for personal illness or to attend to an immediate family member.

2. Employees must use all of their available PTO balance before they can access donated days.

3. Qualifying employees may receive a maximum of fifteen (15) donated PTO days during a school year.

4. Employees may only donate time from their current PTO balance.

5. An employee may donate a maximum of five (5) PTO days to a particular employee in any one school year.

6. All donations must be made in full day increments.

7. Once donated time has been transferred to the recipient's PTO balance, the donor has no rights to that time for any reason. Approved donations will be immediately deducted from the donor's PTO balance and credited to the recipient's balance.

8. The decision to donate PTO should be an individual and personal decision and is completely voluntary.

9. All PTO donations must be approved by the Director. Employees desiring to donate PTO to an employee must submit a written request to the Director indicating the number of days donated, the date of donation, and an acknowledgement of remaining days after the donation. Both the Director and employee will sign the letter of acknowledgement. Requests that do not meet the conditions of this policy will be denied.

10. All donated PTO days must be used for their intended purpose.

11. The Director will coordinate with the School's Management Company to assure proper documentation of these transactions. The Director will notify the donor and the recipient after the transaction has occurred.

# Information Technology Systems Security Plan

Mountain Heights Academy
Adopted: September 27, 2017
Amended: June 14, 2021

## 1. PURPOSE

The primary purpose of this Information Technology Systems Security Plan is to establish security measures that will help Mountain Heights Academy (the "School") protect sensitive data that is stored or maintained on its computer equipment, systems, and networks. The School is required to establish this Plan pursuant to Utah Administrative Code Rule R277-487 and the School's Information Technology Security Policy.

## 2. SCOPE AND APPLICABILITY

This Plan is applicable to employees, volunteers, and third-party contractors of the School. The School will use this Plan to protect its computer equipment, systems, and networks from, among other things, unauthorized access, inappropriate disclosure, and compromise.

This Plan works in conjunction with the School's Information Technology Security Policy, Student Data Privacy and Security Policy, Family Educational Rights and Privacy Policy and Administrative Procedures, Data Governance Plan, and policies and procedures pertaining to the School's electronic resources and devices.

This Plan contains security measures 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

The School's contracted IT provider functions as the School's IT Security Manager and will help the School implement this Plan and comply with it. The responsibilities of the IT Security Manager set forth in this Plan supplement the responsibilities of the IT Security Manager outlined in the School's Data Governance Plan, which 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.

Please refer to the School's Data Governance Plan to review the data privacy and security roles and responsibilities of the School's Student Data Manager, employees, educators, volunteers, and third-party contractors.

## 4. COMPLIANCE

School employees, volunteers, and third-party contractors must comply with this Plan. Failure to comply shall result in consequences for the person or entity up to and including removal of access to the School's computer equipment, systems, and networks. If such access is required for employment or contracted services, employees and third-party contractors may be subject to dismissal.

## 5. REPORTING

All persons who are granted access to the School's computer equipment, systems, and networks are expected to be careful and aware of suspicious communications and unauthorized use of the School's IT assets. When School personnel or other users become aware of suspicious activity, they shall immediately contact the Student Data Manager or IT Security Manager with the relevant information.

## 6. SYSTEM ADMINISTRATION

System administration is a critical function that provides management of the School's information systems that contain sensitive data, including personally identifiable student data. If

malicious actors compromise system administration, they have access to the School's sensitive data and information systems.

The School's information systems will be administered by the IT Security Manager. The IT Security Manager will use a combination of preventative, detective, forensic, and audit controls to protect system administration channels from exploitation by attackers.

**7. NETWORK SECURITY**

It is essential for the School to protect its network from both internal and external malicious actors. The School recognizes that appropriate network security procedures are necessary for identifying, evaluating, controlling, and mitigating network vulnerabilities and for protecting the School's technology assets.

The IT Security Manager will manage the School's network according to industry best practices. In so doing the IT Security Manager will provide a secure and robust computing environment at the School; protect the School's information technology assets and systems; and preserve the privacy of sensitive data belonging to the School's employees, students, and associated entities.

All wireless access networks at the School shall conform to current best practices and shall utilize at minimum WPA encryption for any connections. No wireless access point shall be installed on the School's network that does not conform to current network standards as defined by the IT Security Manager.

The School shall ensure that any remote access with connectivity to the School's internal network is achieved using the School's centralized VPN service that is protected by multiple factor authentication systems.

**8. APPLICATION SECURITY**

Web application vulnerabilities account for the largest portion of attack vectors outside of malware. To help protect the School from harm, it is essential to perform security assessments of web applications used by the School.

The IT Security Manager shall perform a security assessment of all web applications that are used (or will be used) by the School to house sensitive data. The purpose of the security assessments is to identify potential or realized weaknesses. Any vulnerabilities found in a web application used by the School shall be remediated. If serious vulnerabilities in a web application cannot be remediated, the web application shall be removed.

The IT Security Manager shall determine which web application security assessment tools to use.

**9. ENDPOINT, SERVER, AND DEVICE SECURITY**

The School understands the importance of preventing, detecting, and remediating attacks and compromises of the School's computers, servers, and other computing devices.

School employees' computers or computing devices shall not be left unattended and unlocked for extended periods of time, especially when logged into sensitive systems or data, including personally identifiable student or employee data. Automatic log off, locks, and password screen savers should be used to enforce this requirement.

The IT Security Manager shall ensure that all servers at the School undergo a security audit and evaluation before they are used by the School. Administrative access to servers shall be password protected. Any and all new servers must be registered and approved by the IT Security Manager. The maintenance and support of all new servers should be managed by the School's IT Security Manager, if possible.

The School shall install, distribute, and maintain spyware, malware, and virus protection software on all School-owned technology assets, including computers, computing devices, and servers.

Server rooms and telecommunication rooms/closets shall be protected by appropriate access control which segregates and restricts access from general office areas at the School. Access control shall be enforced using keys, electronic card readers, or another similar method. Only IT and other School personnel whose job functions require access to such rooms shall be allowed unescorted access.

Before any third-party contractor is allowed access to any computer system, server room, or telecommunication room, the contractor shall be required to present a company issued identification card and his or her access must be confirmed directly by the School employee who issued the service request or by the IT Security Manager.

**10. IDENTITY, AUTHENTICATION, AND ACCESS MANAGEMENT**

The School shall grant access to its systems and network in accordance with the principles of least privilege and need-to-know. In addition, the School shall require unique identities and authentication in order to access the School's systems and network. This will ensure that users

are identifiable and unable to repudiate their activities on the School's systems and network.

Passwords are a critical component of information security and the school shall enforce strong password management. All individual passwords connected to the use of the School's computer equipment, systems, and networks shall:

1. Be created and maintained in accordance with industry best practices;
2. Be maintained in a manner that reduces the threat of unauthorized access to sensitive data;
3. Be treated as confidential information and not be shared with anyone; and
4. Not be inserted into email messages or any other forms of electronic communication.

Any user suspecting that his or her password may have been compromised shall report the incident to the IT Security Manager and change all passwords.

**11. DATA PROTECTION AND CRYPTOGRAPHY**

One of the most effective ways to achieve data security is through encryption. To read an encrypted file, a person must have access to a secret key or password that enables the person to decrypt it.

Where technologically feasible, the School shall utilize encryption when transmitting sensitive data over the network.

All computers and other computing devices owned by the School, such as desktop computers, laptops, and tablets, that connect to the School's network and that may contain or transmit personally identifiable data must be configured to encrypt such data on any internal hard drive. Users must protect these devices from unauthorized use or access.

Personally identifiable data shall not be stored on external storage media such as external hard drives, flash drives, or DVDs unless such storage is authorized by the Student Data Manager and the personally identifiable data on the external storage media is encrypted. Users must protect these external storage media from unauthorized use or access.

All employees or other users that need assistance or guidance on encrypting sensitive data on any School computer or device described in this section shall contact the IT Security Manager.

## 12. MONITORING, VULNERABILITY, AND PATCH MANAGEMENT

This area is concerned with minimizing the School's attack surface through the detection and mitigation of vulnerabilities and the early detection of intrusions.

The IT Security Manager shall:

1. Monitor the School's network so that it may detect and investigate security incidents when they occur;
2. Engage in effective vulnerability management and penetration testing in order to detect and remediate vulnerabilities when they occur in the School's computer equipment, systems, and applications; and
3. Perform regular patch management in order to maintain the School's information systems in a secure state.

## 13. HIGH AVAILABILITY, DISASTER RECOVERY, AND PHYSICAL PROTECTION

Procedures related to high availability, disaster recovery, and physical protection are intended to make it possible for the School to continue to operate successfully in the face of adversity, which may range from mild, routine failures of School computers to severe natural or man-made catastrophes.

The School will ensure the availability and recoverability of the School's data and data systems in accordance with industry best practices.

Physical access to the School's data centers shall be governed by the same access requirements applicable to server rooms and telecommunications rooms at the School.

## 14. INCIDENT RESPONSES

All incidents of network or system shutdown or failure shall be reported to the IT Security Manager immediately. The IT Security Manager shall utilize industry standards and current best practices in responding to and resolving such incidents.

Incidents involving a data breach shall be reported to the Student Data Manager who, along with the IT Security Manager, shall follow the data breach protocol set forth in the School's Data Governance Plan.

## 15. ACQUISITION AND ASSET MANAGEMENT

The School shall follow its purchasing and procurement policies when purchasing technology equipment.

The School will track, support, and manage all of its acquired technology assets (hardware and software) in a reasonable and effective manner.

## 16. POLICY, AUDIT, AND E-DISCOVERY TRAINING

The School shall provide training on its policies as required by law. This includes providing training to its employees, aids, and volunteers regarding information technology security matters on an annual basis. The School shall also provide training on audits and e-discovery as required by law.

## 17. REVIEWS AND AUDITS

The IT Security Manager shall periodically review the School's security policies, procedures, plans. The IT Security Manager shall ensure that security and privacy audits are performed as required by this Plan or by law.

## Laptop Use Agreement and Acceptable Use Policy for Students

**Mountain Heights Academy**
**Adopted:**

We acknowledge that the technology equipment identified below, together with the associated software, bag, and tag is the property of Mountain Heights Academy and is being assigned to the student only for educational purposes associated with enrollment as a student of the school.

By signing this document, we agree to use the laptop and associated peripherals and software in connection with the student's education with the school and shall not permit any other person to possess or use the laptop or the software. We shall not sell, lease, or otherwise grant anyone rights to the laptop or the software. We shall adhere to the Acceptable Use Policy of the school and comply with all applicable copyright and other regulations regarding the software.

We agree to promptly inform the school of loss or damage of the laptop. In the event of a loss we agree to fully cooperate with the school in preparing any necessary report and in any ensuing investigation. We understand that we are responsible for the full cost of replacing the laptop if it is lost or for the cost of necessary repairs, whether accidental or otherwise.

We acknowledge that the laptop is provided for the student's use only while he or she remains a student of the school. If the student ceases enrollment in the school, we will return the computer to authorized school personnel within seven days or be subject to late fees. The laptop will be returned in the same condition as on the agreement date of issue, reasonable wear and tear excepted, and we understand that we are responsible for the cost to repair any damage, accidental or otherwise. We understand that the removal of any stickers or tags is strictly prohibited and may result in replacement fines. If we fail to return the laptop upon request, the school may treat this as a loss and we understand that we will be responsible to pay the full replacement fee of up to $800.

Mountain Heights Academy makes every effort to issues only laptops with zero damage. However, we also understand that this may not happen 100% of the time. Students and their parents have 48 hours after the date they are issued their laptop to report any damages to the Mountain Heights Academy office. Students and their parents will be asked to complete a laptop damage form and submit it. Any damage not reported in the first 48 hours will be the financial responsibility of the parent.

The Internet can be a valuable and amazing learning tool. However, it can also be used for inappropriate activities. Carefully read the following information that outlines the School's policy on the acceptable use of school computer equipment.

1. No Browsing of Restricted Content Web sites: The School may block access to Web sites which contain pornographic or other obscene or inappropriate material. However, the World Wide Web changes on a daily basis. In this connection, users who find new sites which the School has not yet blocked are required to report such sites to the Administrator or IT representative. Browsing web sites that contain pornographic material is never allowed and doing so will lead to loss of computer privileges or suspension. The first incident will result in a behavior contract with the school and possible suspension. The second incident will result in loss of computer privileges for the remainder of the school year and possible suspension. Also, no student is allowed to view or download pornographic material via the Internet.

   The School may also block access to non-school related sites. If a student requests access to a currently blocked site, prior to being unblocked, it must be vetted by a teacher/administrator to verify that it is necessary for a Mountain Heights Academy course.

2. Downloading of Non-Business Related Data: The School allows the download of files from the Internet. However, downloading files should be limited to those which relate directly to School business. Any student that chooses to download non-School related material does so at their own risk.

3. Downloading of Application Programs: The School recognizes that the dynamic nature of online education may require the download or installation on School computers of application software from the Internet; however such installs will be done remotely

through Mountain Heights Academy IT staff. Students must not attempt to install any software on a school laptop. Such software may not only contain embedded viruses, but also is untested and may interfere with the functioning of standard School applications. Students and their parents will be held financially responsible for any loss or damage resulting from the attempted download or installation of any application or program that has not been conducted with the express assistance of the Mountain Heights Academy IT representative.

4. Participation in Web-based Surveys: When using the Internet, the user implicitly involves the School in his/her expression. Therefore, users should not participate in Web or E-mail based surveys or interviews as a student or under a school login or Internet connection without authorization.

5. Use of Subscription-Based Services: Some Internet sites require that users subscribe before being able to use them. Users should not subscribe to such services as a student or under a school login or Internet connection without the express approval of the Administrator.

6. Violation of Copyright: Many of the materials on the Internet are protected by copyright. Even though they may seem to be freely accessible, many of the intellectual property laws which apply to print media still apply to software and material published on the Internet. Students are permitted to print out Web pages and to access material from the Internet for informational purposes as long as the purpose for such copying falls into the category of "fair use." Please do not copy or share material which is copyrighted, including music files. Students having any questions regarding such materials should contact the Administrator for guidance.

I agree to abide by the Laptop and Acceptable Use Policy. I understand that my Internet activity is monitored on School computers, as is my email account and that I have no expectation of privacy on a School computer. I also understand that I will be held accountable if I violate any part of the Laptop and Acceptable Use Policy, and that violation of this policy may result in the loss of the privilege of using a School computer.

By completing the section below, you are agreeing to the entire contents above in addition to Section H from the Student Handbook outlined below.

H.3 Educational materials (laptop, power cord, laptop bag, lanyard, English novels etc.) will need to be returned to Mountain Heights Academy Salt Lake Office within seven days of any of the following events:

- The school year has ended.
- The student is no longer enrolled in the school, for any reason.
- The materials are damaged and need to be replaced.
- The materials are being repossessed due to a violation of policies outlined in this Handbook.

The parent has seven business days from a qualifying event to return the Mountain Heights Academy educational materials to the SL Office. All equipment shall be in the same condition as delivered with the exception of normal wear and tear. Parents will be responsible for any damage to the materials and will be invoiced for any damages resulting from damage. Failure to comply with these rules will result in financial charges to the parent. If materials are not received the parent/legal guardian is responsible for the cost to replace any missing materials.The failure to complete a timely return of any course materials upon request shall constitute a theft and may result in invoicing, referral to a collections agency, or legal action. Laptop damage and charges may either be assessed during the return process or invoiced afterwards once tech support has been able to thoroughly assess the extent of the damage. Payment in full will be due 30 days from the date of the invoice and may be payable online or via check.Laptop bags should be returned free of stains or smells. A $15.00 cleaning fee will be assessed to any bags that require cleaning. If the bag is damaged beyond repair it is rendered unusable, a $30.00 replacement fee will be charged.

H.4 Technology

A virtual school requires the use of technology to promote and support student learning. All school participants, including parents/legal guardians, students, and staff, will use Mountain Heights Academy's Learning Management System (LMS) and the Internet to communicate and share information.

The school's hardware and software requirements for accessing the LMS can be met by using the equipment provided by the school according to your school's specific Agreement. If you

choose to not use school equipment, you may use your family's personal computer, a computer in a public library, or any other computer so long as the equipment used meets the program's minimum specifications (see the Use of Personal Equipment section). Due to certain licensing restrictions, some of the additional software provided with the school computer may not be available for use on personal computers. For specific questions on particular software licensing issues, media requirements, and determining if your computer meets the minimum requirements, contact Tech Support.

H.4.1 Use of the Learning Management System (LMS)

Regular use of the LMS is required in order to participate in the school. Training on how to use the LMS is provided by the school, and completing this training is required.The LMS is available 24 hours a day, except for periodic maintenance, most of which will occur early Sunday mornings. Users will be notified in advance of any maintenance that is anticipated to disrupt service for an extended period of time.

Security and Privacy

Security and privacy are very important in preserving the integrity of our school. Each LMS user is responsible for keeping his or her username and password confidential. Usernames and passwords should never be provided to anyone (except tech support as needed) at any time. Students may provide this information to their parents/legal guardians; however, parents/legal guardians should use their own login information to access the LMS. Parents and students who experience difficulty in using the LMS should first be sure they have completed any available training and accessed help resources available from their home pages. If they are unable to resolve their problems, they should contact Mountain Heights Academy Tech Support at 801.721.6329 with any technical questions.

H.4.2 Use of Mountain Heights Academy Equipment and Installed Software

Any equipment provided by Mountain Heights Academy is to be used only for school purposes. Mountain Heights Academy will not be responsible for management, recovery or loss of any personal photos, music or e-mails. Email privileges may be revoked at any time

for misuse or abuse. If email is revoked, the user will not be allowed to retrieve saved email or Google docs.

Software

All software settings, default configurations, and administrative privileges will be maintained at the original settings unless a change is authorized by Mountain Heights Academy Tech Support. Mountain Heights Academy equipment contains software that permits remote access to the equipment, permits its use to be monitored, or enables it to be shut down remotely. Personal information is not collected or maintained by Mountain Heights Academy, and any access is only for the purpose of making repairs, verifying acceptable use, or disabling equipment. Each software application provided by Mountain Heights Academy must be used in accordance with the license and/or use agreement that accompanies that software application. Breaking a license agreement is an illegal act and is punishable by law. Under no circumstances can parents/legal guardians/students redistribute any software provided to them by Mountain Heights Academy. Modification of any equipment or software without Mountain Heights Academy's written consent is strictly prohibited and may result in charges for any required repairs and loss of laptop use privileges The Mountain Heights Academy has an administrative account on each computer. Under no circumstance will Mountain Heights Academy provide administrator rights over the system configuration. Users that refuse to provide any required passwords when requested, or tamper with the administrative account access, will forfeit their rights to support services and may lose laptop use privileges. Blocked websites may only be requested for whitelisting by a teacher.

Educational software not provided by Mountain Heights Academy may be requested for installation only if specifically authorized by Tech Support. The decision as to whether to permit the installation is solely determined by the Mountain Heights Academy administration. If the installation of such software, even if authorized, results in any damage to the equipment or software, parents/legal guardians will be responsible for the costs of any repairs. Under no circumstances are repairs to be performed on an Mountain Heights Academy computer by anyone other than Mountain Heights Academy tech support. Users who attempt repairs or take Mountain Heights Academy equipment to a third party for repairs may lose laptop use privileges.

H.4.4 Use of Personal Equipment and Software

Parents/legal guardians may use their own equipment and software as long as they meet the minimum requirements detailed in this section. Mountain Heights Academy has no responsibility for providing any support for equipment that doesn't belong to the school.

SIGNATURE PAGE
MUST BE SIGNED AND TURNED IN BEFORE LAPTOP IS ISSUED

Model _____
Serial Number of Laptop _____
Student Name _____
Student Signature _____
Parent/Guardian Name_____
Parent/Guardian Signature_____
Date _____

# Public Education Engagement and Exit Survey Procedures

Mountain Heights Academy
Adopted: April 22, 2020

Mountain Heights Academy (the "School") recognizes the importance of understanding factors that influence public educator satisfaction and the reasons public educators choose to leave the School or public education in general. The School believes that collecting such information may help the School improve their educators' morale, engagement, and job satisfaction, as well as help the School improve its recruitment and retention of educators.

The School shall abide by Utah Code § 53G-11-304 and Utah Administrative Code Rule R277-325 with respect to the administration of the Public Education Engagement Survey and the Public Education Exit Survey.

The purpose of these administrative procedures is to help the School comply with all requirements related to the surveys as set forth in the law.

## Definitions

"Educator" for purposes of these administrative procedures means:

(a) a general education classroom teacher;

(b) a preschool teacher;

(c) a special education teacher; or

(d) a school based specialist.

"Public Education Engagement Survey" for purposes of these administrative procedures means the model Public Education Engagement Survey referenced in and available at R277-325-3(2)(a).

"Public Education Exit Survey" for purposes of these administrative procedures means the model Public Education Exit Survey referenced in and available at R277-325-3(2)(b).

## Administering Surveys

### Public Education Engagement Survey

The School shall request that its educators complete the Public Education Engagement Survey, at a minimum, every other year beginning in the 2019-20 school year. Except as provided below with respect to new educators, the School shall request that its educators complete the Public Education Engagement Survey in the opposite years from those in which it administers the school climate survey described in Rule R277-623 (for example, if the School administers the school climate survey in the 2020-21 school year, the School should request that its educators complete the Public Education Engagement survey in the 2019-20 school year).

With respect to new educators, the School shall request that its new educators complete the Public Education Engagement Survey every year for the first three years the educator is in the profession.

### Public Education Exit Survey

The School shall request that an educator leaving the School complete the Public Education Exit Survey at the time of the educator's separation from employment with the School.

### Survey Providers

The School shall use a USBE-approved online provider or a provider approved by the LEA to administer the Public Education Engagement Survey and Public Education Exit Survey. If the School administers the Public Education Engagement Survey or the Public Education Exit Survey through a provider other than a USBE-approved online provider, the School shall provide the data from the surveys to the State Superintendent by June 30 annually in a manner prescribed by the State Superintendent.

### Survey Questions

The School may add additional questions to the model Public Education Engagement Survey or Public Education Exit Survey when it administers such surveys to its educators, but any additional questions:

(a) must allow each educator to remain anonymous;
(b) must not request the educator's CACTUS ID number; and
(c) may ask each educator to voluntarily identify the educator's school.

## Survey Results

Only the School's Director, Board of Directors, and appropriate personnel specifically authorized by the Director may have access to results of the Public Education Engagement and Exit Surveys.

The Director shall implement whatever protective measures are necessary to prevent the identification of educators who complete the surveys, including but not limited to:

(a) instructing educators to not share personally identifiable information in their survey responses; and
(b) redacting any personally identifiable information that educators inadvertently (or intentionally) include in survey responses before giving access to the survey results to authorized individuals identified in the paragraph above.

# Religion and Education Policy Procedures

Mountain Heights Academy
Adopted: March 29, 2024
Amended: October 19, 2026

**Purpose**

Mountain Heights Academy (the "School") recognizes, protects, and accommodates the rights of religious practice and expression guaranteed by state and federal laws and by the constitutions of Utah and the United States.

The purpose of this procedure is to help School personnel protect and accommodate individual religious belief and rights of conscience in the School.

**General Rules Regarding Religion and Education**

The School expects School personnel to foster mutual understanding and respect for all individuals and beliefs. Study about religion is an important part of a complete education and is necessary to achieving an understanding of history, societies, and cultures throughout the world. School curricula – including activities, discussions, assignments, displays, and performances – may refer to religious thought and expression, provided such references are designed to achieve specific educational objectives.

School personnel should neither promote nor disparage any religious, agnostic or atheistic belief or religion in general. Teaching about religion should be objective, thus avoiding any implication that religious doctrines have the endorsement of school authority. School personnel should recognize that religious holidays are observed in various ways, or not observed at all, based upon the influence of ethnic tradition, family style, or religious conviction.

The School shall ensure that:

a. a student may express the student's beliefs about religion in homework, artwork, and other written or oral assignments free from discrimination based on the religious perspective of the student's submissions;

b. home and classroom work is:

i. not penalized or rewarded on the basis of religious perspective; and

ii. judged by ordinary academic standards of substance, relevance, and other legitimate pedagogical objectives; and

c. notification of the constitutional freedoms described in these procedures are provided to school officials, employees, and students.

Students may refrain from participation in any aspect of school that violates a religious belief or right of conscience of the student or of the student's parent or guardian.

The School shall not in any aspect of school:

a. require or incentivize a student to affirm or deny the student's or the student's parent or guardian's religious belief or right of conscience;

b. engage a student in a practice that violates or is contrary to the student's or the student's parent or guardian's religious belief or right of conscience; or

c. penalize or discriminate against a student for refraining from participation due to the student's or the student's parent or guardian's religious belief or right of conscience.

A student's parent or guardian may waive the student's participation in any aspect of school (e.g., activities, discussions, and assignments) that the parent or guardian feels would violate the parent or guardian's or student's rights of conscience or religious belief. Such waivers must be communicated in a timely manner to the appropriate School authorities.

**Procedures for Implementation**

1. The Director will periodically review these procedures with teachers and staff. This review will stress the School's expectation that School personnel will recognize, protect, and accommodate religious belief and individual rights of conscience in the operation of the School, while fostering mutual understanding and respect for all individuals and beliefs.

2. The School encourages teachers and employees at the School to discuss, equitably and with civility, and, if possible, resolve with students, parents, and guardians, any concerns regarding curricular content, activities, or student participation.

3. Students, parents, and legal guardians will be provided with a copy of these procedures annually through the posting of these procedures on the School's website

4. A student, or parent or legal guardian of any student, may make a complaint to the Director that a portion of the curriculum, a School activity, or the conduct of a School employee violates state or federal law insofar as it "endorse[s], promote[s], or disparage[s] a particular religious, denominational, sectarian, agnostic, or atheistic belief or viewpoint." See Utah Code § 53G-10-202(4).

5. The Director may discuss annually with the Board any requests for accommodation, or complaints about religion in the curriculum, made within the last year. In discussing these matters with the Board, the Director will take care to protect the privacy rights of those who made complaints or requests.

**Waivers of Participation**

1. When a student refrains from participating in any aspect of school that violates the student's or the student's parent or guardian's religious belief or right of conscience, the School:

a. Shall promptly notify the student's parent or guardian;
b. May offer an alternative that does not violate the student's or the student's parent or guardian's religious belief or right of conscience; and
c. May not require the student or the student's parent to explain, defend, or justify the student's or the student's parent or guardian's religious belief or right of conscience.

2. In addition, if a student refrains from a portion of a course or to a course in its entirety under Utah Code § 53G-10-205, the parent and School may work together to establish an alternate academic accommodation, which allows the student to demonstrate mastery of Core Standards or alternate standard, consistent with Utah Code § 53G-6-803(7) and Utah Code § 53G-10-205(2)(b).

3. When a student's parent or guardian waives the student's participation in any aspect of school that the parent or guardian feels would violate the student's or the student's parent or guardian's religious belief or right of conscience, the parent or guardian shall communicate that waiver (preferably in writing) as soon as possible to the Director so that an appropriate alternative for the student can be considered.

4. The School will keep, for a reasonable time, a written record of every waiver of participation based on religious belief or right of conscience.

### Complaints Alleging Violation of Law

Any student, parent, or legal guardian may register a complaint with the Director that a particular curriculum or activity violates state or federal law insofar as it endorses, promotes, or disparages a particular religious, denominational, sectarian, agnostic, or atheistic belief or viewpoint.

If a complaint is made by a minor student, the Director will give written notice to the student's parent or legal guardian by email to the parent or legal guardian's last known email address.

The Director, student, the student's parent or legal guardian, and the teacher or employee responsible for the program in question will meet to discuss the complaint, and the Director will arrive at a decision, consistent with state and federal law, whether to alter the curriculum or activity, substitute another activity, or deny that the curriculum or activity is in violation of law. The Director will give a written decision as soon as practical under the circumstances.

The School will keep, for a reasonable time, a written record of every complaint and any decisions made regarding each complaint.

### Appeals Process

A student, parent, or legal guardian who is dissatisfied with a Director's decision regarding complaints about curricula and activities perceived to be in violation of law, may appeal that decision within ten (10) days to the Board President.

The Board President will review the complaint of the student, parent, or legal guardian and the decision of the Director and may modify the Director's decision.

At the sole discretion of the Board President, a committee of his or her choosing may be formed to review the complaint and the decision of the Director. If the Board President decides to form a committee to consider the appeal, the student and student's parent or guardian will be notified.

The Board will keep, for a reasonable time, a written record of every appeal and any decisions made regarding each appeal. The decision of the Board President will be final.

# Student Education Plan Procedures

**Mountain Heights Academy**
**Adopted: August 6, 2021**

These procedures are established in accordance with the Student Education Plan Policy adopted by the School's Board of Directors.

1. Plans for College and Career Readiness

   (a) The School shall develop and maintain a plan for college and career readiness (also known as a CCR) for each of its students in grades 7-12. The purpose of such plans is to support the educational and occupational preparation of the students. A student's plan for college and career readiness shall:

      (i) Be initiated at the beginning of the student's 7th grade year;
      (ii) Be collaboratively developed by the student, the student's parent or guardian, and School personnel (such as School counselors, teachers, or administrators);
      (iii) Identify the student's skills and objectives;
      (iv) Map out a strategy to guide a student's course selection; and
      (v) Link the student to post-secondary options, including higher education and careers.

   (b) Plans for college and career readiness shall be developed at individual and group conferences. The School shall invite parents or guardians to attend and participate in individual conferences. Upon request, the School shall provide reasonable accommodations in connection with the conferences. The School shall hold conferences as follows:

      (i) For students in grades 7-8, hold at least one group conference and one individual conference during the two school years;
      (ii) For students in grades 9-10, hold at least one group conference and one individual conference during the two school years; and
      (iii) For students in grades 11-12, hold at least one group conference and one individual conference during the two school years

(c) At the individual and/or group conferences, School personnel shall plan, monitor, and help manage the student's education and career development by doing at least the following:

(i) Include and engage the student's parents or guardians, where possible;
(ii) Celebrate the student's strengths and accomplishments;
(iii) Review the student's courses, future course options, and progress toward meeting Utah's student achievement standards and applicable graduation requirements;
(iv) Review the student's objectives and goals and discuss areas where the student could improve; and
(v) Discuss and evaluate the student's post-secondary higher education and career options.

(d) In the event the School receives Comprehensive Counseling and Guidance funds, the School shall comply with R277-462 with respect to plans for college and career readiness. This includes, but is not limited to, having students prepare a four-year plan at the beginning of their 7th grade year or within the first year they are enrolled in grades 7-12; including parents or guardians in individual planning meetings with their students; having plans maintained by the School's counseling department; having plans follow a student as the student progresses through each grade; having plans transfer with students between LEAs, when applicable; and holding individual and group conferences as outlined in the rule.

# Time and Effort Documentation Procedures

Mountain Heights Academy
Adopted: October 23, 2020

**Purpose**

1. All employees paid in whole or in part with federal funds, and employees whose salaries are used to meet a matching/cost sharing requirement, are required to provide time and effort documentation that accurately/reasonably represents the work that has been performed during the period being reported on.

    a. **Semi-Annual Certification** – This certification must be submitted by/for employees who spend 100% of their time and effort on a single federal program during the six-month period being reported on.

        i. Semi-Annual Certifications will be submitted for the periods July 1 through December 31, and January 1 through June 30.

        ii. Semi-Annual Certifications must be submitted after the last day of the period being reported (after the fact).

        iii. Semi-Annual Certifications must be submitted on an approved form.

        iv. Forms will include:

            1. Name of Employee.

            2. Title of Employee.

            3. Period being reported on.

            4. A certification statement stating the employee has spent 100% of their time on the stated program.

            5. Name of the program worked on.

6. Whether time, effort and salary are being used for cost sharing or matching purposes. If so, for which program(s).
7. Signature of Employee.
8. Date Signed by Employee (Note: Cannot be dated prior to the end of the period covered by the certification).
9. Signature and Title of Direct Supervisor.
10. Date Signed by Supervisor (Note: Cannot be dated prior to the end of the period covered by the certification).

b. **Personnel Activity Report (PAR)** – This report must be submitted by/for employees that:

   i. Meet at least one of the following criteria:

      1. Work on multiple federal awards.
      2. A federal award and a non-federal award.
      3. Employees that work on a single federal award, but are paid for indirect cost activities AND direct cost activities.
      4. Employees that work on two or more indirect cost activities that are allocated using two different allocation bases.
      5. An employee that works on a federal award but on an unallowable activity and a direct or indirect cost activity.

   ii. PARs will be submitted on a monthly basis.

   iii. PARs must be submitted after the last day of the month being report on (after the fact).

   iv. PARs must be submitted using an approved form.

   v. Forms will include:

1. Employees Name.
2. Period being reported on (e.g., January 1 through January 31, 2020).
3. A certification statement stating that the distribution of the employee's time is an accurate representation of the work performed.
4. Whether time, effort and salary are being used for cost sharing or matching purposes. If so, for which program(s).
5. Distribution of time (by percentage e.g., 70% Title I, 30% SpEd) by account, Function, Program, Location.
6. Time being reported must represent but cannot exceed 100%.
7. Must coincide with one or more pay periods.
8. Signature of Employee.
9. Date Signed by Employee (Note: Cannot be dated prior to the end of the period covered by the PAR).
10. Signature and Title of Direct Supervisor
11. Date Signed by Supervisor (Note: Cannot be dated prior to the end of the period covered by the PAR).
12. Sick time, vacation time, etc. must be coded proportionally to the different programs.

2. Payroll records must reconcile with the time and effort documentation.
3. A reconciliation of payroll records and time and effort documents will be done on a quarterly basis. Adjustments will be made and discussed, as necessary.
4. If an employee's salary is being used for cost sharing/matching purposes, then this needs to be identified on the employee's time and effort certification form. Once a

salary has been used for matching purposes or a portion of the salary, then the salary, or portion thereof, that has been used may not be used as matching/cost sharing funds for another program.

5. If assignments change, it is the School's responsibility to inform the School's business administrator so that payroll records, budgets, etc. can be updated.
6. Upon termination of employment, an employee must submit their final time and effort documentation prior to receiving their final payment.
7. Procedures will be periodically reviewed by the administration. Updates due to changes in rules or regulations will be made in a timely manner, as necessary.
8. Employees will receive appropriate training on time and effort documentation.
9. The School will keep a copy of all time and effort documentation (Semi-Annual Certifications, Personnel Activity Reports, payroll reports, etc.) in accordance with the School's record retention practices or 5 years, whichever is greater (See 2 CFR 200.333).