

**Wallace Stegner Academy  
Administrative Procedures Manual**

**Last Revised: August 20, 2018**

---

# TABLE OF CONTENTS

---

Administration of Medication Procedures.....	3
Arrest Reporting Procedures .....	6
Attendance Procedures .....	8
Background Check Procedures.....	12
Carbon Monoxide (CO) Response Plan .....	15
Child Abuse and Neglect Reporting Procedures .....	17
Concussion and Head Injury Procedures.....	20
Data Confidentiality Addendum .....	24
Data Governance Plan.....	27
Driving Procedures.....	42
Electronic Resources Procedures .....	44
Emergency Drill Form.....	55
Emergency Response and Preparedness Plan .....	55
Family Education Rights and Privacy Procedures .....	57
Free and Reduced Price Policy .....	63
Certification of Acceptance Submission .....	63
Hazardous Materials Procedures .....	68
Hiring Procedures .....	69
Home and Hospital Request Forms .....	70
Human Sexuality Instruction Procedures.....	72
Information Technology Systems Security Plan .....	74
Meal Charge and Alternate Meal Procedures.....	80
Religion and Education Procedures .....	84
Safety Procedures.....	87
Snow and Ice Removal Procedures .....	88
Student Data Disclosure Statement .....	89
Student Injury Reporting Procedures.....	91
Volunteer Procedures.....	92

---

## **Administration of Medication Procedures**

These procedures are established in accordance with the Administration of Medication Policy adopted by the School's Board of Directors.

### Administration of Medication by School Personnel

In order to ensure safe administration of medication to students, the procedures outlined here must be followed.

- (1) The Principal will designate a reasonable number of School employees who will be responsible for administering medication to students in the School.
  - (2) The Principal will arrange for the Principal and all designated School employees to receive adequate training from a licensed health care professional prior to administering any medication. Training should include indications for the medication, means of administration, dosage, adverse reactions, contraindications, and side effects.
  - (3) The student's parent or guardian must complete the parent/guardian section of the Student Medication Form requesting that medication be administered to the student during regular school hours. Parents are responsible for updating the Student Medication Form as necessary.
  - (4) The student's health care provider must complete the Health Care Provider section of the Student Medication Form indicating the child's name, the name of the medication, the purpose of the medication, the means of administration, the dosage, the time schedule for administration, the anticipated number of days the medication needs to be given at school, and possible side effects. The practitioner must also affirm that giving the medication during school hours is medically necessary.
  - (5) A Student Medication Log must be maintained for any student who has medication administered at school, and all employees authorized to administer medication will be notified regarding each student to whom they are authorized to administer medication.
  - (6) Each time medication is given, the person who gave it must document the administration in ink on the Student Medication Log. If the medication is not administered as scheduled, a notation must be made on the Student Medication Log as to why the medication was not given, and the student's parent or guardian must be notified.
  - (7) The Student Medication Form and Student Medication Log will be retained in the student's records.
  - (8) Teachers of the student receiving medication during school hours will be notified.
  - (9) Medication (other than that carried by a student) must be delivered to the School by the student's parent or guardian or designated adult.
-

(10) Medication should be delivered to the School in a container properly labeled by a pharmacy, manufacturer or health care provider. Labeling must include the student's name, the name of the prescribing practitioner, date the prescription was filled, name and phone number of the dispensing pharmacy, name of the medication, dose, frequency of administration, and the expiration date.

(11) Medication must be stored in a secure, locked cabinet or container in a cool, dry place, except that:

- a. medications that require refrigeration must be stored appropriately;
- b. insulin or emergency medications such as EpiPens, Twinject Auto-Injectors, asthma inhalers and glucagon must not be stored in a locked area so that they are available when needed.

(12) Authorization for administration of medication by School personnel may be withdrawn by the School at any time following written or verbal notice to the student's parent or guardian, as long as this action does not conflict with federal laws such as IDEA and/or section 504 of the Rehabilitation Act. The Principal may withdraw authorization for administration of medication in cases of noncompliance or lack of cooperation by parents or students unless the student's right to receive medication at school is protected by laws such as IDEA or section 504.

### Self-Administration of Medication by Students

Students may possess and self-administer prescription medication if:

(1) The student's parent or guardian signs a statement:

- a. Authorizing the student to self-administer the medication; and
- b. Acknowledging that the student is responsible for, and capable of, self-administering the medication; and

(2) The student's health care provider provides a written statement

- a. That it is medically appropriate for the student to self-administer the medication and be in possession of the medication at all times; and
- b. Containing the name of the medication prescribed for the student's use.

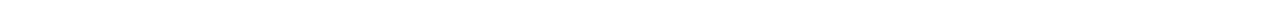
The School will provide an acceptable form for parents to request that their student be allowed to possess and self-administer prescription medication.

### Application of Sunscreen

---

Students may possess and self-apply sunscreen without a parent or physician's authorization.

If a student is unable to self-apply sunscreen, a school employee may apply the sunscreen on the student if the student's parent or legal guardian has provided written consent.



# **Arrest Reporting Procedures**

These procedures are established in order to comply with the Arrest Reporting Policy adopted by the School's Board of Directors.

## **Required Reports**

(a) Non-USOE-licensed employees of the School, (b) Board Members, and (c) any School employees who drive a motor vehicle as part of their employment responsibilities must report to the Principal information regarding the following matters:

- Convictions, including pleas in abeyance and diversion agreements;
- Any matters involving arrests for alleged sex offenses;
- Any matters involving arrests for alleged drug-related offenses;
- Any matters involving arrests for alleged alcohol-related offenses; and
- Any matters involving arrests for alleged offenses against the person under Title 76, Chapter 5 (i.e., assault, battery, etc.)

## **Timeline for Reports**

Current employees of the School must provide the required reports to the Principal within seven (7) days of receiving notification of this policy from the Principal. Thereafter, employees of the School must submit required reports to the Principal within seven (7) days of the event necessitating the report. New employees of the School must report this information prior to commencing work for the School.

## **Procedure for Review of Reports**

The Principal will review and investigate all reports received pursuant to the policy and determine whether any employment action is necessary to protect the safety of students.

The Principal will maintain the confidentiality of the information submitted and only share such information with individuals who have a legitimate need to know. Information regarding the reports, the results of any investigation, the Principal's determination and any action taken will be maintained in a separate, confidential employment file. These records will only be kept as long as the Principal determines it is necessary to protect the safety of students.

## **Required Action**

Any individual who reports a matter involving alleged sex offenses or other alleged offenses which may endanger students shall be immediately suspended from all student supervision responsibilities during the period of investigation.

Any individual who reports a matter involving alcohol or drugs shall be immediately suspended from transporting students, operating motor vehicles on school business, or operating or maintaining school vehicles during the period of investigation.

---

## **Training**

The Principal will ensure that individuals subject to this policy receive appropriate training regarding their arrest reporting obligations.

---

# Attendance Procedures

These procedures are established in accordance with the Attendance Policy established by the School's Board of Directors.

## Definitions

**"Absence"** means a student's nonattendance at school for one school day or part of one school day.

**"Valid excuse"** or "excused absence" means an absence resulting from:

- a) an illness;
- b) a death of a family member or close friend;
- c) a documented medical appointment;
- d) a family emergency;
- e) an approved school activity;
- f) a preapproved extended absence for a family activity or travel, consistent with school policy; or
- g) an absence permitted by an individualized education program or accommodation plan, developed pursuant to relevant law.

The Principal has the discretion to consider other absences as "valid excuses."

**"Habitual truant"** means a school-age minor who: (1) is at least 12 years old; (2) is subject to the requirements of Section 53A-11-101.5; and (3)(a) is truant at least ten times during one school year; and (b) fails to cooperate with efforts on the part of school authorities to resolve the minor's attendance problem as required under Section 53A-11-103.

**"Truant"** means absent from school without a valid excuse.

**Attendance Requirements:** Students are allowed a maximum of five (5) unexcused absences per year.

**Excused Absences:** An oral or written communication documenting a valid excuse must be received from the student's parents/guardian within one (1) business day of the absence in order for the absence to be excused. In the event of multiple consecutive absences, written communication must be received within one (1) business day of the student's return to school.

In the event of an unforeseeable illness or emergency, the School should be notified as soon as reasonably possible.

Excused absences may become unexcused if the Principal determines that absences have reached an excessive level and are adversely impacting the student's education.

**Preapproved Extended Absence:** A parent/guardian may request approval from the principal prior to a student's extended absence of up to ten (10) days per school year. The principal will approve the absence if the principal determines that the extended absence will not adversely impact the student's education.

---

**Make-up Work:** Make-up work is permitted for students who have excused absences. The teacher will provide the student or the parent/guardian with any make-up work upon request. Make-up work must be completed within a reasonable time-frame as determined by the teacher.

**Tardiness:** A student is tardy if he or she is not in the assigned classroom when the late bell rings. In general, tardiness will be handled on an individual basis with the teacher. If a student is chronically tardy, then the student may be referred to the administration. Elementary students are allowed five (5) tardies per quarter. Middle school students are allowed three (3) tardies per class each quarter.

**Notification of Absences and Tardies:** In the event a student is absent, parents/guardians will be notified by phone on the day of the absence. Parents and students are responsible for tracking the total number of absences and tardies. Parents will be notified when their student reaches the 4<sup>th</sup> unexcused absence of the year. Parents of elementary students will be notified when their child is tardy for the 4<sup>th</sup> time during a given quarter. Parents of Middle School students will be notified if their child is tardy for the 2<sup>nd</sup> time in a class for the given quarter. If the maximum limit for unexcused absences or tardiness is reached, the principal will attempt to schedule a meeting with the parents to review the situation and will outline the appropriate corrective action.

**Grounds for an Appeal:** Students who believe that all or part of their absences and/or tardies should be considered excused may provide a written request to the administrator to review their case.

### **Notice of Compulsory Education Violation**

The School may issue a "notice of compulsory education violation" to a parent/guardian of a student who is under the age of fourteen (14) if the student is truant at least five (5) times during the school year.

This notice shall:

1. Direct the parent/guardian to meet with School authorities to discuss the student's attendance problem and cooperate with the principal and Board to secure regular attendance by the student;
2. Designate the School authorities with whom the parent is required to meet;
3. State that it is a class B misdemeanor for the student's parent or guardian to intentionally or recklessly fail to meet with the designated school authorities to discuss the student's attendance problems, or fail to prevent the student from being truant an additional five (5) more times during the remainder of the school year; and
4. Be served on the parent/guardian by personal service or certified mail.

### **Truancy Intervention Program**

The School's Truancy Intervention Program is established to encourage good attendance and to facilitate the processing of chronically truant students through the juvenile court.

---

Those efforts will include documented earnest and persistent efforts to resolve a student's attendance problems as follows:

- Annual notification of the School's attendance policies will be provided to the parents of all students at the time of registration.
- When a student's attendance is negatively affecting the student's learning, the classroom teacher will notify the student and/or the student's parent(s) of the concern. The teacher will set up a conference with the student and/or the student's parent(s) to identify and resolve any problems that prevent the student from attending school. The student's progress will be monitored.
- If meeting with the student and parent(s) does not adequately address the problems and the student's learning continues to suffer, then the school counselor or principal will work with the teacher and parent(s) in finding a solution to the problems that are preventing the student from attending to his/her learning. Efforts to resolve the problems may include, but are not limited to, the following: making adjustments to the curriculum or the schedule, counseling of the student by school authorities, considering alternatives proposed by the parent, or providing the parent with a list of community resources to help the family.
- The principal may consult with a parent/guardian to determine if mitigating circumstances such as medical or psychological problems indicate the use of intervention methods for resolving the attendance problems.
- In the event that the preceding interventions fail, a certified letter will be sent to the parent(s) requesting a formal meeting with the administrator to resolve the attendance problems. A copy of the letter and mailing certificates will be kept by the School.
- The principal will notify the student and a parent/guardian of the actions the School may take should the student be truant in the future.

### **Habitual Truancy Citation**

Consistent with Section 53A-11-101.7, a habitual truancy citation may be issued to a student who is a habitual truant.

Habitual truancy citations will only be issued after the School has made earnest and persistent efforts to resolve student attendance problems, which efforts may include those set forth above.

Habitual truancy citations will be served on the parent/guardian by personal service or certified mail. The parent/guardian will have the right to appeal a truancy citation in writing to the principal within ten (10) days of being issued.

The School will refer a student to whom a habitual truancy citation has been issued to juvenile court. A court referral will include a recommended disposition containing the following: [a] documentation of attendance and academic achievement; [b] documentation of school efforts to improve attendance; [c] copies of truancy citations, including all mailing certificates; and [d] student background as requested by the prosecuting agency.

---



## **Background Check Procedures**

These procedures are established pursuant to the Background Check Policy established by the School's Board of Directors.

### Individuals Subject to Background Checks

The School requires that the following individuals submit to a criminal background check and ongoing monitoring as provided in Utah Code § 53A-15-1503 as a condition for employment or appointment: (a) each new non-USOE-licensed employee; (b) each volunteer who will be given significant unsupervised access to a student in connection with the volunteer's assignment; (c) each employee of a staffing service who works at the School; and (d) each Board Member.

Additionally, each new employee who is licensed by the Utah State Office of Education ("USOE") must obtain a background check and submit to ongoing monitoring as required in connection with USOE's licensure requirements.

By September 1, 2018, the School will collect the information described below from individual who were employed by the School prior to July 1, 2015, and with whom the School maintains an authorizing relationship and submit that information to the Utah Bureau of Criminal Identification for ongoing monitoring.

### Conducting the Background Check

Any person submitting to a background check for the School will sign a waiver notifying the individuals (a) that a criminal background check will be conducted, (b) who will see the information received as a result of the background check, and (c) how that information will be used.

The School will collect the following from an individual required to submit to a background check for the School:

- (a) personal identifying information, including but not limited to:
  - (i) current name, former names, nicknames, and aliases;
  - (ii) date of birth,
  - (iii) address,
  - (iv) telephone number,
  - (v) driver license number or other government-issued identification number,
  - (vi) social security number, and
  - (vii) fingerprints;
- (b) a fee as set forth below;
- (c) consent and waiver on a form specified by the School for the background check acknowledging that their fingerprints are being registered for ongoing monitoring by the School.

The School will submit such individuals' personal identifying information, including fingerprints, to the Utah Bureau of Criminal Identification for an initial background check

---

and ongoing monitoring (if the results of the initial criminal background check do not contain disqualifying criminal history information as determined by the School).

### Ongoing Monitoring

The School will request that the fingerprints taken for the purpose of conducting criminal background checks be registered with any rap back system maintained to provide ongoing status notifications to the School of any criminal history reported on individuals whose fingerprints are registered in the system.

### Payment of Fee for Background Check

Applicants for employment, including substitutes, shall be required to pay the designated costs of background checks subject to the provisions of Utah Code Ann. § 53A-15-1503(2).

The School shall pay the cost of the background check for current non-licensed employees and volunteers of the School.

The School will not pay the cost of fingerprinting for School employees or volunteers.

### Background Check Evaluation

When making decisions regarding employment or appointment based on the information received from a criminal background check, the School will consider:

- (a) any convictions, including pleas in abeyance;
- (b) any matters involving a felony; and
- (c) any matters involving an alleged:
  - (i) sexual offense;
  - (ii) class A misdemeanor drug offense;
  - (iii) offense against the person under Title 76, Chapter 5, Offenses Against the Person;
  - (iv) class A misdemeanor property offense that is alleged to have occurred within the previous three years; and
  - (v) any other type of criminal offense, if more than one occurrence of the same type of offense is alleged to have occurred within the previous eight years.

Only those convictions which are job-related for the employee, applicant, or volunteer will be considered by the School.

### Opportunity to Respond to Background Check

The School will provide an individual an opportunity to review and respond to any criminal history information received as a result of submitting for a criminal background check or through ongoing monitoring.

---

If a person is denied employment or appointment or is dismissed from employment or appointment because of information obtained through a criminal background check or ongoing monitoring, the person may request a review of the information received and the reasons for the disqualification and shall be provided written notice of the reasons for denial or dismissal and of the individual's right to request a review of the disqualification.

### Confidentiality

Information received by the School as a result of a background check will only be (a) available to individuals involved in the hiring or background investigation process for that individual and (b) used for the purpose of assisting the School in making employment-related decisions. Any person who disseminates or uses any such information for any other purpose is subject to criminal penalties and civil liability as set forth in applicable law.

### Privacy Risk Mitigation Strategy

The School will employ reasonable privacy risk mitigation strategies to ensure that the School only receives notifications for individuals with whom the School maintains an authorizing relationship. Specifically, upon (a) termination of an employee's employment with the School, (b) expiration of a Board Member's term without renewal, or (c) resignation of Board Member, the administration will ensure that the School's management company receives notification of the event. The School's management company will take any steps necessary to terminate ongoing monitoring for such individuals and will document the date on which such steps were taken. For volunteers, the School's management company will establish a schedule to review the volunteers registered for ongoing monitoring for the School, consult with School personnel to determine whether such individuals are still volunteering for the School, and terminate ongoing monitoring for individuals as appropriate.

---

## Carbon Monoxide (CO) Response Plan

Carbon Monoxide (CO) is a colorless, tasteless and odorless gas that is slightly less dense than air. It becomes toxic to humans when levels reach high levels as it displaces oxygen required for life and inhibits oxygen uptake by those exposed to the gas. It is a byproduct of combustion and can be present if heaters and other fuel consuming appliances malfunction. For this reason CO detectors are installed within classrooms and areas where natural gas or other fuel is used most commonly for heating purposes (HVAC, water heaters, etc.).

The CO detectors are located throughout the building and tie directly back to the building's fire panel located in the front office. A monitoring company also monitors the detectors remotely as individual zones. Alarms generated by detectors will cause a blue strobe light to flash in the area of detection and will also cause the panel to sound. The steps for responding to alarms are outlined below.

Because the CO detectors in the building detect any amount of CO and can give false alarms due to dust or other contaminants on the detector it may be difficult to distinguish a true alarm where occupants are in danger from a false alarm triggered by a faulty detection. The detectors only determine the presence of CO: they do not indicate the concentration or if levels have reached a dangerous level. CO is common in small amounts in the atmosphere and is even a byproduct of some normal biological functions. In very small amount the gas poses no risk of toxicity. While every alarm is important to investigate, it is also important to understand the need to avoid panic.

Upon receipt of a CO alarm the fire panel will sound and alert the remote monitoring company. The remote monitoring company will call all parties listed on the predetermined emergency contact list. The school Director or administrator in charge should immediately call Academica West's assigned maintenance person to investigate the alarm. The alarm can be silenced at the panel in the front office by pressing the silence or acknowledge button.

The building will operate as normal by not evacuating staff, students and patrons at this time unless symptoms of poisoning are evident (see symptom list below and follow steps accordingly). If a technician cannot arrive at the site within thirty minutes of the received alarm the local fire department will be contacted and dispatched to the site to check for high levels of carbon monoxide.

When the Academica West Maintenance person or Fire Department arrives at the site they will go to the location of the tripped detector and begin measuring for high CO levels in that area and surrounding areas. If CO levels greater than 50 ppm are detected the building will be evacuated immediately following the same procedure as outlined in the school fire evacuation plan.

Upon any required CO evacuation the following entities will be notified:

- Local fire department
  - Natural gas utility/Questar
-

- Wallace Stegner Academy Directors
- Academica West Facilities Personnel

If high levels of CO are not found the affected CO detector will be examined and replaced (if needed) by a certified technician and the system restored to normal operation.

If an alarm has sounded and over a short period of time several occupants have complained of symptoms similar to the following, the area and building should be evacuated immediately, following the established emergency evacuation plan.

Symptoms may include:

- Dull Headache
- Weakness
- Dizziness
- Nausea or vomiting
- Shortness of breath
- Fluttering or throbbing heartbeat
- Red skin complexion
- Confusion
- Blurred vision
- Fainting
- Loss of Consciousness

The school staff should contact 911 and the appropriate authorities. If not on the premises, the school staff should call and notify the school Directors and administration. The school should call and notify Academica West.

School staff will ensure those experiencing symptoms are moved to an area of fresh air and receive prompt medical attention.

All students will be accounted for in the event of an evacuation and the school will notify families of the situation and the steps that will be taken to resume a school day or release students back to their guardians.

---

## Child Abuse and Neglect Reporting Procedures

These procedures are established pursuant to the Child Abuse and Neglect Reporting Policy adopted by the Board of Directors.

1. If a School employee **has reason to believe** that a child may have been subjected to incest, molestation, sexual exploitation, sexual abuse, physical abuse, or neglect, or observes a child being subjected to conditions or circumstances which would reasonably result in such, the employee shall immediately make an oral report to the nearest peace officer, law enforcement agency or Division of Child Family Service (“DCFS”) and to the School’s Principal.

a. The oral report may be made with the Principal present, but the person making the report must be present.

b. The reporting employee must record the name of the individual and the agency contacted to make the required report.

c. The reporting employee must complete and provide a copy of the Child Abuse and Neglect Reporting Form to the Principal within twenty four (24) hours. The Principal will keep the form in a separate file, and it shall not be placed in the student’s permanent file. The form should also be sent to the agency to which the oral report was given.

d. The Principal will preserve the anonymity of the person making the report and any others involved in any investigation.

2. To determine whether or not there is **reason to believe** that abuse or neglect has occurred, school employees may (but are not required to) gather information only to the extent necessary to determine whether a reportable circumstance exists.

a. Investigations by staff prior to submitting a report shall not go beyond what is minimally necessary to support a reasonable belief that a reportable problem exists.

b. It is not the responsibility of the Principal or any other school employees to prove who the abuser is or that the child has been abused or neglected, or to determine whether the child is in need of protection.

c. School employees shall not contact the parents, relatives, friends, neighbors, etc. for the purpose of determining the cause of the injury and/or apparent neglect.

d. School employees shall not conduct interviews with the child or contact the suspected abuser.

e. Notes of voluntary or spontaneous statements by the child shall be given to the investigational agency.

---

3. Investigations of reports of abuse for children seventeen (17) years of age and younger are the responsibility of DCFS.

a. School employees shall not contact the child's parents, relatives, friends, neighbors, etc. for the purpose of determining the cause of the injury and/or apparent neglect.

b. The Principal may provide the child's parents with a basic notification of the alleged incident and that a report has been made to DCFS/law enforcement. The parents should then be told that they will receive any/all additional information about the investigation from DCFS.

c. If school officials are contacted by parents about child abuse reports, school personnel shall not confirm or deny that a contact or investigation is taking place. A school employee should refer the caller to law enforcement or DCFS.

d. School officials shall cooperate with DCFS and law enforcement employees authorized to investigate reports of alleged child abuse and neglect.

4. If the suspected perpetrator of child abuse or neglect is a School employee, the Principal shall immediately report the allegation to the Utah State Office of Education. Steps shall be taken to assure that further abuse or neglect is prevented by the suspected perpetrator.

5. Persons making reports or participating in good faith in an investigation of alleged child abuse or neglect are immune from any civil or criminal liability that otherwise might arise from those actions.

7. The Principal shall provide each School employee with annual training and/or the written Child Abuse and Neglect Reporting Policy including a copy of the Child Abuse and Neglect Reporting Form. Newly hired staff will be provided with the same training and/or written policy at the beginning of their employment. The training and/or distribution of materials will be documented.

---

\*\*\*CONFIDENTIAL\*\*\*

### Child Abuse and Neglect Reporting Form

Oral report made to Principal: Date: \_\_\_\_\_ Time: \_\_\_\_\_

**Child's Information:**

Name: \_\_\_\_\_ Age: \_\_\_\_\_ Birth Date: \_\_\_\_\_ Sex: \_\_\_\_\_  
Address: \_\_\_\_\_

**Parent/Guardian Information:**

Father Name: \_\_\_\_\_  
Father Address: \_\_\_\_\_  
Father Telephone: \_\_\_\_\_  
Mother Name: \_\_\_\_\_  
Mother Address: \_\_\_\_\_  
Mother Telephone: \_\_\_\_\_  
Guardian/Caretaker Name: \_\_\_\_\_  
Guardian/Caretaker Address: \_\_\_\_\_  
Guardian/Caretaker Telephone: \_\_\_\_\_

**Circumstances leading to the suspicion that the child is a victim of abuse or neglect:** \_\_\_\_\_  
\_\_\_\_\_

Time and date of observations: \_\_\_\_\_  
Additional information: \_\_\_\_\_  
\_\_\_\_\_

**Oral report made to:**

Agency: \_\_\_\_\_  
Individual's Name: \_\_\_\_\_  
Date: \_\_\_\_\_ Time: \_\_\_\_\_

**Written report sent to:**

Agency: \_\_\_\_\_  
Individual's Name: \_\_\_\_\_  
Date: \_\_\_\_\_ Time: \_\_\_\_\_

**Reporting Individual:**

Name: \_\_\_\_\_  
Signature: \_\_\_\_\_  
Date: \_\_\_\_\_

**Principal:**

Name: \_\_\_\_\_  
Signature: \_\_\_\_\_  
Date: \_\_\_\_\_

**Do not place this form in the student's file.**

## Concussion and Head Injury Procedures

These procedures are established pursuant to the Concussion and Head Injury Policy established by the School's Board of Directors.

A concussion is a type of traumatic brain injury that interferes with normal function of the brain. It occurs when the brain is rocked back and forth or twisted inside the skull as a result of a blow to the head or body. What may appear to be only a mild jolt or blow to the head or body can result in a concussion. A concussion can occur even if a player or student in an activity is not knocked out or loses consciousness.

The School will ensure that each agent of the School is familiar with, and has a copy of, the Concussion and Head Injury Policy and these Procedures. Before permitting a child to participate in a sporting event of the School, the School will:

- (a) provide a written copy of the Concussion and Head Injury Policy and these Procedures to a parent or legal guardian of a child; and
- (b) obtain the signature of a parent or legal guardian of the child, acknowledging that the parent or legal guardian has read, understands, and agrees to abide by, the Concussion and Head Injury Policy and these Procedures.

The following definitions apply to these Procedures:

- (1) "Agent" means a coach, teacher, employee, representative, or volunteer.
  - (2) "Qualified health care provider" means a health care provider who:
    - (a) is licensed under Title 58, Occupations and Professions; and
    - (b) may evaluate and manage a concussion within the health care provider's scope of practice.
  - (3) "Sporting event" means any of the following athletic activities that is organized, operated, managed, or sponsored by the School:
    - (a) a game;
    - (b) a practice;
    - (c) a sports camp;
    - (d) a physical education class;
    - (e) a competition; or
    - (f) a tryout.
  - (4) "Traumatic head injury" means an injury to the head arising from blunt trauma, an acceleration force, or a deceleration force, with one of the following observed or self-reported conditions attributable to the injury:
    - (a) transient confusion, disorientation, or impaired consciousness;
    - (b) dysfunction of memory;
    - (c) loss of consciousness; or
    - (d) signs of other neurological or neuropsychological dysfunction, including:
      - (i) seizures;
      - (ii) irritability;
      - (iii) lethargy;
      - (iv) vomiting;
      - (v) headache;
      - (vi) dizziness; or
-

(vii) fatigue.

The following signs and symptoms following a witnessed or suspected blow to the head or body are indicative of probable concussion:

Signs (observed by others):

- Student appears dazed or stunned
- Confusion
- Forgets plays
- Unsure about game, score, opponent
- Moves clumsily (altered coordination)
- Balance problems
- Personality change
- Responds slowly to questions
- Forgets events prior to hit
- Forgets events after the hit
- Loss of consciousness (any duration)

Symptoms (reported by student):

- Headache
- Fatigue
- Nausea or vomiting
- Double vision, blurry vision
- Sensitive to light or noise
- Feels sluggish
- Feels “foggy”
- Problems concentrating
- Problems remembering

The School will (a) immediately remove a child from participating in a sporting event of the School if the child exhibits signs, symptoms, or behaviors consistent with a concussion or is otherwise suspected of sustaining a concussion or a traumatic head injury; and (b) prohibit the child from participating in a sporting event of the School until the child:

(i) is evaluated by a qualified health care provider who is trained in the evaluation and management of a concussion; and

(ii) provides the School with a written statement from the qualified health care provider described in Subsection (1)(b)(i) stating that:

(A) the qualified health care provider has, within three years before the day on which the written statement is made, successfully completed a continuing education course in the evaluation and management of a concussion; and

(B) the child is cleared to resume participation in the sporting event of the School.

The school will follow any return-to-play guidelines established by the student’s qualified health care provider.

---

## **Emergency Procedures**

The following situations constitute a medical emergency and require notification of emergency medical personnel:

- (1) Any student with a witnessed loss of consciousness (LOC) of any duration should be spine boarded and transported immediately to nearest emergency department via emergency vehicle.
- (2) Any student who has symptoms of a concussion, and who is not stable (i.e., condition is worsening), should be transported immediately to the nearest emergency department via emergency vehicle.
- (3) A student who exhibits any of the following symptoms should be transported immediately to the nearest emergency department, via emergency vehicle:
  - a. Deterioration of neurological function
  - b. Decreasing level of consciousness
  - c. Decrease or irregularity in respirations
  - d. Any signs or symptoms of associated injuries, spine or skull fracture, or bleeding
  - e. Mental status changes: lethargy, difficulty maintaining arousal, confusion or agitation
  - f. Seizure activity

A student who is symptomatic but stable may be transported by his or her parents. The parents should be advised to contact the student's primary care provider or seek care at the nearest emergency department on the day of the injury.

## **Guidelines and Procedures for Coaches and Teachers Supervising Contests and Games**

### *Recognize concussion*

1. All agents of the school should become familiar with the signs and symptoms of concussion that are described above.
2. Agents of the school shall have appropriate training about recognizing and responding to traumatic head injuries, consistent with the employees' responsibilities for supervising students and athletes.

### *Remove from activity*

Any student who exhibits signs, symptoms, or behaviors consistent with a concussion (such as loss of consciousness, headache, dizziness, confusion, or balance problems) shall be immediately removed from the sporting event and shall not return to play until cleared by an appropriate health care professional.

### *Refer the athlete/student for medical evaluation*

---

1. The school's agent is responsible for notifying the student's parent(s) of the injury.
    - a. Contact the parent(s) to inform a parent of the injury. Depending on the injury, either an emergency vehicle will transport or parent(s) will pick the student up at the event for transport.
    - b. A medical evaluation is required before returning to play.
  2. In the event that a student's parent(s) cannot be reached, and the student is able to be sent home (rather than directly to a doctor):
    - a. The school's agent should ensure that the student will be with a responsible individual who is capable of monitoring the student and understanding the home care instructions before allowing the student to go home.
    - b. The school's agent should continue efforts to reach a parent.
    - c. If there is any question about the status of the student, or if the student cannot be monitored appropriately, the student should be referred to an Emergency Department for evaluation. An agent of the school should accompany the student and remain with the student until a parent arrives.
    - c. The school's agent shall provide for supervision of other students for whom he or she is responsible when accompanying the injured student.
-

## Data Confidentiality Addendum

This Data Confidentiality Addendum (the “Addendum”) is entered into this \_\_\_\_ day of \_\_\_\_\_, 20\_\_, between **Wallace Stegner Academy**, a Utah nonprofit corporation (“School”), and \_\_\_\_\_ (“Contractor”).

### Recitals

- A. School and Contractor are parties to a contract (the “**Contract**”) regarding products and/or services to be provided and/or licensed by Contractor to School (the “**Contractor Services**”).
- B. Utah Code § 53A-1-1410 establishes requirements for contracts between educational entities such as School and third party contractors such as Contractor.
- C. The parties are entering into this Addendum, in order to ensure that the agreement between the parties complies with Section 53A-1-1410.

### Agreement

Now, therefore, in consideration of the foregoing and the mutual covenants and promises of the parties hereto, the parties agree as follows:

- 1. Except as provided in Utah Code § 53A-1-1410(4), Contractor will not use any personally identifiable student data received from School for any purpose other than to provide the Contractor Services to School.
    - a. “Personally identifiable student data” means student data that identifies or is used by the holder to identify a student and includes:
      - i. a student’s first and last name;
      - ii. the first and last name of a student’s family member;
      - iii. a student’s or a student’s family’s home or physical address;
      - iv. a student’s email address or other online contact information;
      - v. a student’s telephone number;
      - vi. a student’s social security number;
      - vii. a student’s biometric identifier;
      - viii. a student’s health or disability data;
      - ix. a student’s education entity student identification number;
-

- x. a student's social media user name and password or alias;
  - xi. if associated with personally identifiable student data, the student's persistent identifier, including:
    - 1. a customer number held in a cookie; or
    - 2. a processor serial number;
  - xii. a combination of a student's last name or photograph with other information that together permits a person to contact the student online;
  - xiii. information about a student or a student's family that a person collects online and combines with other personally identifiable student data to identify the student; and
  - xiv. other information that is linked to a specific student that would allow a reasonable person in the school community, who does not have first-hand knowledge of the student, to identify the student with reasonable certainty.
2. Contractor acknowledges that all student data of the School is the property of the student under Utah Code § 53A-1-1405. Contractor will collect, use, store, and share personally identifiable student data only in accordance with the Contract, this Addendum, Utah Code § 53A-1-1410, as it may be amended, and any administrative rules adopted by the Utah State Board of Education. The parties acknowledge and agree that the terms of Utah Code § 53A-1-1410, as it may be amended, and any administrative rules adopted by the Utah State Board of Education implementing Utah Code § 53A-1-1410 govern the relationship between the parties.
3. Contractor may only share personally identifiable student data with employees and independent contractors of Contractor who have a legitimate need to such data in order to enable Contractor to provide the Contractor Services to School. School may request that Contractor notify School of independent contractors with whom Contractor shares such data and the purpose for which such data is shared and to verify to School that such independent contractors are bound by confidentiality agreements similar in scope to this Addendum.
4. At the request of School, Contractor will allow School or its designee to audit Contractor in order to verify compliance with the terms of the Addendum that relate to the confidentiality and protection of personally identifiable student data. This right to conduct an audit is subject to Contractor's confidentiality obligations to other customers and third parties.
-

5. During the term of the Contract, Contractor will delete personally identifiable student data at the request and direction of School.
6. At the completion of the parties' agreement, if the Contract has not been renewed, Contractor shall return or delete upon the School's request all personally identifiable student data of the School in Contractor's possession and provide to the School written verification of the return or deletion of such data, including deletion from Contractor's back-up system.
7. The Contractor covenants and agrees that it shall defend School from and against any and all third party claims related to the unauthorized disclosure of Personally Identifiable Student Data by Contractor or its employees, agents, officers and directors, and indemnify School against any final judgements entered by a court of competent jurisdiction, and associated legal fees.
8. In the event of any conflict between the Addendum and the Contract, the terms of this Addendum shall govern.

The parties have executed this Addendum as of the date first set forth above.

**Wallace Stegner Academy**, a Utah non-profit corporation

\_\_\_\_\_  
Name: \_\_\_\_\_  
Title: \_\_\_\_\_

**Contractor:**

\_\_\_\_\_

\_\_\_\_\_  
Name: \_\_\_\_\_  
Title: \_\_\_\_\_

# Data Governance Plan

## 1. PURPOSE

Wallace Stegner 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 Principal 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, Movelt (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 fulfill 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 the School's 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. Information related to the Utah Registry of Autism and Developmental Disabilities;
22. 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));
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;
8. Information requested in Household Application for Free and Reduced Price School Meals, including data related to household members, whether any household members participate in assistance programs (such as SNAP, TANF, or FDPIR), and household income;

**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 yellow immunization card from the state, other proof of immunizations, or an Immunization Exemption Waiver;
3. If applicable, a copy of a student's IEP, IHCP, or Section 504 Plan;
4. Proof of a vision exam for students under 8 years of age entering school for the first time in Utah;
5. 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;
6. A copy of a transfer student's record from the student's previous school;
7. Fee Waiver Application, as applicable;
8. Household Application for Free and Reduced Price School Meals, 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 registration) is stored electronically by the School in Aspire, which is the student information system provided to Utah schools by the USBE. Aspire provides a secure location for the storage, maintenance, and transmission of student data. If the School chooses to use any additional student information systems, it will ensure that the system has adequate security protections. School employees and volunteers shall not store personally identifiable student data on their personal computers or devices, flash drives, or any other removable data storage media unless authorized by the Student Data Manager.

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

---

**6.3 Third-Party Contractors.** Third-party contractors shall store personally identifiable student data received from the School only in accordance with their contract and Data Confidentiality Addendum 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;
  - 3. Grade Level;
  - 4. Participation in officially recognized activities and sports;
  - 5. Degrees, honors, and awards; and
  - 6. Parent names and contact information.
-

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 and Expungement.** The School shall retain and dispose of student records in accordance with Utah Code Ann. § 63G-2-604, Utah Code Ann. § 53A-1-1407, and rules adopted by the USBE. The School shall comply with the active retention schedules for student records published by the Utah Division of Archives and Records Service, including the School District General Records Retention Schedule.

The School shall expunge student data in accordance with Utah Code Ann. § 53A-1-1407. In accordance with Utah Code Ann. § 53A-1-1407 and rules adopted by the USBE, the School shall expunge a student's student data that is stored by the School upon request of the student if the student is at least 23 years old. However, the School may not expunge a student's grades, transcripts, record of enrollment, or assessment information. The School may expunge other student data, including a student's medical records and behavioral assessments. A student's parent may also request that the School expunge the student's student data. A request to expunge a student's data shall be made in writing to the School's Principal and describe in detail the data requested to be expunged.

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

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

## **9. DATA BREACH**

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

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

1. Hackers gaining access to personally identifiable student data through a malicious attack (such as phishing, virus, bait and switch, keylogger, denial of service, etc);
-

2. A School employee losing School equipment on which personally identifiable student data is stored (such as a laptop, thumb drive, cell phone, etc) or having such equipment stolen;
3. An unauthorized third party retrieving personally identifiable student data from a School's physical files;
4. A School employee accidentally emailing personally identifiable student data to an unauthorized third party; or
5. A School employee or third-party contractor saving files containing personally identifiable student data in a web folder that is publicly accessible online.

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

#### **9.4 Responding to a Data Breach.**

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

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

1. Lock down systems and data that have been breached or suspected to have been breached, including changing applicable passwords, encryption keys, locks, etc;
  2. Assemble a Data Breach Response Team, which could include the Student Data Manager, IT Security Manager, School employees, Board members, members of the School's management company, the School's IT provider, etc;
  3. Record as many details about the data breach as possible, including:
    - a. Date and time data breach was discovered;
    - b. Data elements involved (for example, students' first and last name, SSIDs, DOBs, passwords, account information, employee social security numbers, etc);
    - c. Data systems involved (for example, Aspire or other School data system); and
-

- d. Type of data breach (physical, such as stolen/lost paperwork or computer equipment; or electronic, such as hacking or unauthorized email transmission).
4. Assign an incident manager that has the appropriate qualifications and skills to be responsible for the investigation of the data breach;
  - a. Investigate scope of data breach to determine types of information compromised and number of affected individuals; and
  - b. Investigate the data breach in a way that will ensure that the investigative evidence is appropriately handled and preserved;
5. Attempt to retrieve lost, stolen, or otherwise compromised data;
6. Determine whether notification of affected individuals is appropriate and, if so, when and how to provide such notification; notification timeframes and requirements should be identified as soon as possible and notices developed and delivered to affected individuals and agencies in accordance with regulatory mandates and timeframes;
7. If the data breach involved the release of a student's personally identifiable student data, notify the student (if the student is an adult student) or the student's parent or legal guardian if the student is not an adult student in a manner reasonable under the circumstances;
8. If the data breach 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.

---

# Driving Procedures

## Purpose

The School takes seriously the safety of its people. The purpose of these procedures is to help ensure the safety of School employees, students, and volunteers. These procedures apply to all employees who operate motor vehicles as part their employment responsibilities and all volunteers who operate vehicles as part of school-sponsored activities.

## Procedures

### Procedures for All Drivers

- The School will perform driver's license verification checks on all new employees and volunteers who operate vehicles on School business.
- The School will verify the driver's license status of driving employees and volunteers at least annually.
- Employees and volunteers who do not have a valid driver's license are not allowed to drive on School business.
- The School will maintain the confidentiality of the results of driver's license checks by ensuring that only designated individuals conduct those checks and that any documentation regarding the results will be maintained in a location where only designated employees have access.
- When driving is an essential function of a job, the School will ensure that job descriptions for such positions specify that maintaining valid drivers license is required.
- Employees and volunteers that are involved in an at-fault accident may not drive on School business until they complete a driver safety program approved by the Principal.
- Employees and volunteers must operate vehicles on School business only within limits of their individual licenses.
- Individuals convicted of DUI or reckless driving may not drive on School business.
- When private vehicles will be used by employees or volunteers on School business,
  - Vehicles must have in effect liability insurance with a minimum of \$100,000 liability coverage.
  - Vehicles must be safe and be in good working order.
  - The Authorization to Use Privately Owned Vehicles on School Business form must be completed by the drivers and owners of the private vehicles and signed by the Principal.

### Additional Procedures for Volunteers Transporting Students

---

In addition to the foregoing procedures that apply to all drivers, the following procedures should be followed when volunteers are transporting students:

- The School will attempt to obtain commercial transportation for students to school-sponsored events whenever possible.
  - Students other than a driver's own children may not be transported in 12 or 15 passenger vans.
  - If the School is unable to obtain commercial transportation and is instead relying on volunteers to transport students to a school-sponsored event, only volunteers approved by the Principal may transport students other than their own children.
  - Parents and students who are being transported to school-sponsored activities by volunteers should sign an informed consent and waiver and release prior to the event.
-

# Electronic Resources Procedures

These procedures are established in order to comply with and implement the Electronic Resources Policy adopted by the School's Board of Directors.

## Electronic Devices

### Definitions

**“Electronic Devices”** means electronic media, communication devices, transmitters, receivers or players, including but not limited to mobile phones with or without video or picture-taking capability, electronic music or video players, iPods, tablets, iPads, and electronic gaming devices.

**“School day”** means the hours that make up the School day according to the School's schedule.

**“School-sponsored activities”** means field trips, curricular and extracurricular activities, and extended School-sponsored trips or activities, including School-provided transportation to and from such activities.

**“Instructional time”** means the hours during the School day designated by the School for class instruction.

### Student Use of Electronic Devices

Electronic devices may only be possessed and used by students during the School day and during School-sponsored activities in accordance with the following standards:

- Electronic devices may not be used to view, access, download, store, or transmit pornography or other obscene or inappropriate material.
- Electronic devices may not be used to bully, threaten, embarrass, harass, or intimidate other students, teachers, volunteers, School guests, or School employees.
- Electronic devices may not be used during quizzes, tests, and standardized assessments except as otherwise provided herein.
- Electronic toys are not allowed in the School.
- Students may have electronic devices at School during the School day.
- Electronic devices must remain out of sight in a bag or backpack and be turned off during the School day.
- Students may not use or respond to electronic devices during instructional time or during other times designated by teachers or the Principal.

### Exceptions

---

The Principal may give permission for a student to possess an electronic device for good cause, including medical reasons, if the device does not distract from the instructional or educational process and is not otherwise used inappropriately.

Parents may request that the Principal allow a student to possess an electronic device on active mode at all times during the School day, with the exception of during tests and standardized assessments, for good cause, including medical needs or unusual family situations.

A student may possess an electronic device on active mode at all times during the regular School day, including during assessments, if such an accommodation is specified in a written Section 504 plan, an Individualized Education Plan, or in connection with other legitimate circumstances determined by the Principal.

Electronic devices may be used in the event of an emergency during the limited period of the emergency in order to protect the safety of a student or School employee, visitor or volunteer.

Parents may make other individualized requests for exceptions to this policy to the Principal.

### **Consequences for Violation**

A student will receive one warning prior to discipline for violating this policy unless the violation involves cheating or constitutes a violation of the School's Safe Schools Policy or Bullying and Hazing Policy or at the discretion of the Principal. On the second violation of this policy, a privately-owned electronic device will be confiscated, labeled, and held in a secure location. The Principal, teachers, and other individuals designated by the Principal may confiscate privately-owned electronic devices under this policy.

*An individual other than a student that finds or confiscates a privately-owned electronic device may search the device for the purpose of determining the device's owner. Students may not search electronic devices. Electronic devices that are used inappropriately may be subject to search by the Principal if there is a reasonable suspicion that the device contains obscene or pornographic material or has been used to cheat or to threaten, embarrass, harass, or intimidate other students, teachers, volunteers, School guests, or School employees.*

The School is not responsible for loss, damage or theft of any privately-owned electronic devices. The School will make reasonable efforts to notify parents/guardians that the School has a student's electronic device in its possession. Parents/guardians who show identification may retrieve confiscated electronic devices during School hours or by appointment. *The School will retain un-retrieved electronic devices until the end of the School year, at which time the devices will be disposed of in a manner that ensures that no data stored on the device may be retrieved.*

---

The Principal may impose additional disciplinary consequences for a student's violation of this policy, considering the nature of the violation and other disciplinary actions in which the student has been involved. Such disciplinary actions may include:

- Loss of the privilege to possess or use electronic devices
- Disciplinary letter to the student's parent/guardian that is placed in the student's file
- Detention
- In-School suspension
- Suspension
- Expulsion
- Loss of the privilege of participating in School-sponsored activities or of receiving honor recognition

The School may contact law enforcement if School employees believe that a student has used an electronic device in connection with a violation of criminal law, and criminal penalties may arise from inappropriate use of electronic devices.

### **Notice of the Policy**

The School will give parents and students written notice of this policy annually. Written notice may be satisfied by posting the policy on the School's website, publishing the policy in a School handbook, sending the policy to the student's home, or any other reasonable means.

### **Creative and Innovative Uses for Electronic Devices**

Teachers and other School employees are encouraged to use electronic devices creatively in order to effectively communicate with students and parents/guardians and to enhance instruction. Creative uses might include notifying absent students of assignments, communicating with parents when students excel or if they are behind or absent, notifying students and parents of news articles or events that would enhance the learning experience, providing feedback to students on tests and assignments, parents notifying the School when students are absent or tardy.

### **Other Provisions**

Picture taking or sound or video recording by students is prohibited in School unless authorized by a teacher or the Principal. Picture taking or sound or video recording by students is prohibited in private areas of the School such as locker rooms, counseling sessions, washrooms, and dressing areas.

Students bring electronic devices on School property at their own risk. The School is not responsible for lost, stolen or damaged electronic devices.

Students are responsible for their own electronic devices and may be subject to discipline if their device is misused by another.

---

Parents, guests and visitors to the School may use electronic devices at School and at School-sponsored activities only in accordance with rules established by the Principal. Such individuals who use the School's electronic resources may not use such resources to access inappropriate material or information.

## **Internet Safety**

The School has established a policy to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act (section 254(h) of title 47, United States Code).

### **Definitions**

Key terms are as defined in the Children's Internet Protection Act.

**"Technology Protection Measure"** means a specific technology that blocks or filters Internet access to visual depictions that are:

- 1- Obscene, as that term is defined in section 1460 of title 18, United States Code.
- 2- Child Pornography, as that term is defined in section 2256 of title 18, United States Code; or
- 3- Harmful to minors.

**"Harmful to Minors"** means any picture, image, graphic image file, or other visual depiction that:

- 1- Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
- 2- Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
- 3- Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

**"Sexual Act"** and **"Sexual Contact"** have the meanings given such terms in section 2246 of title 18, United States Code.

---

### **Access to Inappropriate Material**

To the extent practical, the School will employ technology protection measures (or “Internet filters”) to block or filter Internet access to—or other forms of electronic communications containing—inappropriate information over the School’s network or by School-owned electronic devices.

Specifically, as required by the Children’s Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes. Procedures for disabling or otherwise modifying any technology protection measures shall be the responsibility of the Principal or designated representatives.

### **Inappropriate Network Usage**

To the extent practical, steps shall be taken to promote the safety and security of users of the School online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children’s Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called “hacking” and other unlawful activities and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

### **Education, Supervision and Monitoring**

It shall be the responsibility of all School employees to educate, supervise and monitor appropriate usage of the School’s online computer network and access to the Internet in accordance with this policy, the Children’s Internet Protection Act, the Neighborhood Children’s Internet Protection Act, and the Protecting Children in the 21<sup>st</sup> Century Act. This includes educating students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, as well as cyberbullying awareness and response. The School will also provide information regarding these matters to parents/guardians.

## **Student Acceptable Use of School Electronic Resources**

The School makes various electronic resources available to students. These resources include computers and other electronic devices and related software and hardware as well as the School’s network and access to the Internet. The School’s goal in providing such electronic resources to students is to enhance the educational experience and promote the accomplishment of the School’s mission.

---

Electronic resources can provide access to a multitude of information and allow communication with people all over the world. Along with this access comes the availability of materials that may be considered inappropriate, unacceptable, of no educational value, or even illegal. The School has initiated safeguards to restrict access to inappropriate materials, and use of the Internet and other electronic resources is monitored as well.

In order to use the School's electronic resources, students must be willing to abide by the rules of acceptable use. Use of the School's electronic resources is a privilege, and students have no expectation of privacy in connection with their use of the School's electronic resources. Students who abuse this privilege by actions such as damaging the School's electronic resources; violating copyrights; bullying, hazing, intimidation, harassment and threats; accessing pornography or other obscene or inappropriate material; inappropriate language; gambling; unauthorized games; or other unauthorized or inappropriate use, will be subject to discipline. Violation of policies and rules regarding use of the School's electronic resources may also result in confiscation of School-issued devices and denial of access to the School's electronic resources. This may result in missed assignments, inability to participate in required assignments and assessments, and possible loss of credit or academic grade consequences.

The School may contact law enforcement if School employees believe that a student has used School electronic resources in connection with a violation of criminal law, and criminal penalties may arise from inappropriate use of electronic resources. This applies to use of the School's electronic resources at any time and place, whether on or off School grounds.

Students are personally responsible for School electronic resources provided to them and the students and their parents/guardians may be held responsible for loss or damage to such electronic resources.

Parents play an important role in helping students understand what does and does not constitute acceptable use.

The School may establish agreements for students to sign acknowledging that they understand the rules for use of the School's electronic resources.

### **Staff Acceptable Use of School Electronic Resources**

These procedures apply to employees' and volunteers' use of the School's electronic resources, and employees must agree to these terms as a condition of employment.

---

### **At-Will Employment**

Nothing in this policy is intended to create additional rights for any employee or to otherwise alter or amend the at-will nature of the employment relationship between the School and any employee.

### **The School's Rights**

It is the School's policy to maintain an environment that promotes safe, ethical and responsible conduct in all activities involving the use of the School's electronic resources. The School recognizes its legal and moral obligation to protect the well-being of students and to preserve the integrity of its electronic resources. The School's rights in connection with its electronic resources include but are not limited to the following:

1. All data, files, programs, and materials downloaded with or used, sent, received, or stored upon the School's electronic resources are the School's property, and the School may deal with such items as it deems appropriate.
2. The School may log network use and monitor server space utilization by users and assumes no responsibility or liability for files deleted due to violation of server space allotments.
3. The School may remove a user account on the network with or without notice.
4. The School may monitor all user activities on the School's electronic resources, including but not limited to real-time monitoring of network activity and/or maintaining a log of Internet activity for later review.
5. The School may provide internal and external controls of network usage as appropriate and feasible, including but not limited to restricting online destinations through software or other means.
6. The School may limit or restrict, with or without notice, access to the School's electronic resources for those who do not abide by this policy or other direction governing the use of the School's electronic resources.
7. The School may determine, in its sole discretion, what materials, files, information, software, communications, and other content or activity are permitted or prohibited.
8. The School may delete or remove, with or without notice, any files, programs, data or other materials from any of the School's electronic resources.
9. The School may provide additional policies or guidelines regarding acceptable use of electronic resources.

### **Employees' Responsibilities Regarding Students' Use of Electronic Resources**

Employees who supervise students, control electronic resources, or otherwise have the ability to observe student use of School electronic resources are responsible for educating students on appropriate use of the School's electronic resources. Such employees shall make reasonable efforts to monitor such use to ensure that it is consistent with applicable rules. Employees should make reasonable efforts to become familiar with the Internet and the use of the School's electronic resources to help ensure effective monitoring, instruction, and assistance.

---

## **User Responsibilities**

Use of the School's electronic resources is a privilege intended to help employees fulfill their responsibilities and promote the School's mission. In order to maintain this privilege, users must agree to comply with this policy. Users who are aware of any violation of this policy by any employee must report the violation to the Principal. Employees are responsible for any School electronic resources issued to them at all times and may be held responsible for any inappropriate use, regardless of the user.

Employees may use privately-owned electronic devices at School or at School-sponsored activities in accordance with rules and procedures established by the Principal.

Violation of this policy is grounds for discipline, up to and including termination. The School may also notify law enforcement as appropriate, and such actions may subject an employee to criminal penalties.

## **Acceptable Use**

Standards for acceptable use of the School's electronic resources include but are not limited to the following:

1. All use of the School's electronic resources, including but not limited to use of computers and other electronic devices, use of e-mail, and network and Internet access must be consistent with the School's mission.
  2. Network accounts are to be used only by the authorized user of the account for the authorized purpose.
  3. Users must take reasonable steps to protect the privacy of students, School employees and other members of the School community and must strictly maintain the confidentiality of information regarding such individuals.
  4. Use of the School's electronic resources, whether inside or outside the School, must comply with the School's employee handbook, as established from time to time.
  5. Employees must comply with applicable copyright laws, ethical rules, and other applicable laws and regulations.
  6. Users must exercise appropriate professional judgment and common sense when transporting files to and from school, keeping in mind copyright and other legal issues, as well as ensuring that the non-School computers to or from which files are being transferred are employing appropriate virus-control technologies.
  7. Users must exhibit professionally appropriate behavior when using the School's electronic resources in order to professionally represent and preserve the image the School.
  8. Users must take reasonable precautions to protect the School's electronic resources in order to reduce repair costs, maintain the integrity of the network, and protect the School's assets. Employees who damage School electronic resources may be financially responsible for the cost of repair or replacement.
  9. From time to time, the School will make determinations on whether specific uses of the School's electronic resources are consistent with the intent of this policy.
-

## **Unacceptable Use**

The following uses of the School's electronic resources are prohibited:

1. Excessive use of the School's electronic resources for personal matters. "Excessive use" includes but is not limited to use of electronic resources in a manner that interferes with an employee's performance of work-related responsibilities or with the functioning of the School's electronic resources.
  2. Use of the School's electronic resources in connection with social networking sites for non-academic purposes is prohibited.
  3. Use of the School's electronic resources for commercial or for-profit purposes.
  4. Use of the School's electronic resources for product advertisement or political lobbying.
  5. Personal electronic devices may only be connected to the School's network with appropriate authorization.
  6. Intentionally seeking information on, obtaining copies of, or modifying files, other data, or passwords belonging to other users, or impersonating or misrepresenting other users of the School's network.
  7. Unauthorized use or disclosure of personal student information in violation of the Family Educational Rights and Privacy Act, 34 CFR, Part 99.
  8. Use of the School's electronic resources in a manner that disrupts the use of the network by others.
  9. Destroying, modifying, or abusing the School's electronic resources in any way.
  10. Use of the School's electronic resources in a manner that threatens or impairs the integrity or security of the network.
  11. Use of the School's electronic resources for hate mail, chain letters, harassment, discriminatory remarks, and other antisocial behaviors.
  12. Downloading or installation of any software, including shareware and freeware, for use on the School's electronic resources without the approval of the Principal or designee.
  13. Use of any software on the School's electronic resources in violation of the applicable license or use agreement.
  14. Use of the School's electronic resources to access, process, store, send or receive pornographic, sexually explicit or otherwise inappropriate material (as determined by the Principal).
  15. Use of the School's electronic resources for downloading entertainment software, files or other material not related to the mission of the School. This prohibition pertains to freeware, shareware, copyrighted commercial and non-commercial software, and all other forms of software and files not directly related to the instructional and administrative purposes of the School.
  16. Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner, except that duplication and/or distribution of materials for educational purposes is permitted when such duplication and/or distribution would fall within the Fair Use Doctrine of federal copyright law.
  17. Use of the School's electronic resources for any unlawful purpose.
-

18. Use of the School's electronic resources to intentionally access, process, store, send or receive materials containing profanity, obscenity, racist terms, or other harassing, abusive, intimidating, threatening, discriminatory or otherwise offensive language or images.
19. Use of the School's electronic resources for playing games unless it is for instructional purposes or otherwise approved by the Principal or designee.
20. Participating in activities, including but not limited to the preparation or dissemination of content, which could damage the School's professional image, reputation and/or financial stability.
21. Permitting or granting access to the School's electronic resources, including but not limited to granting use of an e-mail or network account or password, to another individual, including but not limited to someone whose access has been denied or terminated.
22. Portable data storage devices may only be used to backup or transport files and data between computers and use of such devices for the operation of unauthorized portable applications is prohibited.
23. Establishing connections to live communications, including text, voice, or video, may only be done in a manner approved by the Principal or designee.
24. Malicious use of the School's electronic resources to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system.

### **Disclaimer**

1. The School cannot be held responsible for information that is retrieved via the network.
2. Pursuant to the Electronic Communications Privacy Act of 1986 (18 U.S.C. § 2510, et seq.), notice is hereby given that there are no facilities provided by the School's system for sending or receiving private or confidential electronic communications. System administrators have access to all mail and will monitor messages. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.
3. The School is not responsible for any damage users may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions caused by the School's negligence or your errors or omissions.
4. Use of any information obtained is at the user's own risk.
5. The School makes no warranties (expressed or implied) with respect to:
  - The content of any advice or information received by a user, or any costs or charges incurred as a result of seeing or accepting any information;
  - Any costs, liability, or damages caused by the way the user chooses to use his or her access to the network.
6. The School reserves the right to change its policies and rules at any time.

### **Privacy**

Use of and access to the School's electronic resources is provided to employees as a tool for the School's business. The School reserves the right to monitor, inspect, copy, review,

---

store or remove, at any time, without prior notice, any and all usage of the School's electronic resources such as the network and the Internet, including but not limited to e-mail, as well as any and all materials, files, information, software, electronic communications, and other content transmitted, received or stored in connection with this usage. All such information, content, and files are the property of the School. Employees should have no expectation of privacy regarding them. Network administrators may review files and intercept communications for any reason, including but not limited to maintaining system integrity and ensuring employees are using the system consistently with this policy.

---

# Emergency Drill Form

## Fire and Evacuation Drill Observer's Report

*Instructions: Please fill out report for each drill. Keep reports onsite for future State Fire Marshall Inspection.*

Drill Date:	Drill Time:
Drill Location:	Type of Drill <input type="radio"/> Planned <input type="radio"/> False Alarm

List location (if more than one building per school)

---

Scenario or special circumstances:

---

---

Was alarm heard throughout the building? Yes \_\_\_ No \_\_\_

Were all alarm devices operating correctly? Yes \_\_\_ No \_\_\_

If no, note locations \_\_\_\_\_

Did all occupants evacuate the building? Yes \_\_\_ No \_\_\_

If no, note room numbers \_\_\_\_\_

Did occupants assemble in designated areas? Yes \_\_\_ No \_\_\_

Please rate the overall effectiveness of the drill:

Speed of Evacuation Good \_\_\_ Fair \_\_\_ Poor \_\_\_

Effectiveness of Procedures Good \_\_\_ Fair \_\_\_ Poor \_\_\_

Communication during Drill Good \_\_\_ Fair \_\_\_ Poor \_\_\_

Total time required to evacuate building: \_\_\_\_\_ Minutes \_\_\_\_\_ Seconds

Additional comments:

---

---

Time "All Clear" given:	Alarm system reset by:
Observer report completed by:	

**Emergency Response and Preparedness Plan**

---

[Available Separately]

# Family Education Rights and Privacy Procedures

These procedures are established pursuant to the Board's Family Educational Rights and Privacy Policy

## Activities Prohibited without Prior Written Consent

### Prior Written Consent Requirement

Any School employee or agent who plans to administer to a student in any grade any psychological or psychiatric examination, test, or treatment, or any survey, analysis or evaluation that has the purpose or evident intended effect of causing the student to reveal information, whether the information is personally identifiable or not, concerning the student's or any family member's:

- (a) political affiliations or, except as provided under Utah Code § 53A-13-101.1 or rules of the Utah State Board of Education, political philosophies;
- (b) mental or psychological problems;
- (c) sexual behavior, orientation, or attitudes;
- (d) illegal, anti-social, self-incriminating, or demeaning behavior;
- (e) critical appraisals of individuals with whom the student or family member has close family relationships;
- (f) religious affiliations or beliefs;
- (g) legally recognized privileged and analogous relationships, such as those with lawyers, medical personnel, or ministers; or
- (h) income, except as required by law;

shall obtain prior written consent from the student's parent or guardian at least two (2) weeks before the test/treatment/survey/analysis/evaluation is administered or the information listed above is sought, unless the employee or agent must seek this type of private information due to an emergency, or unless a student spontaneously discloses the information.

The prohibitions also apply within the curriculum and other School activities.

### Parental Notice and Consent Checklist

In order to be valid, written parental notice and consent shall include the following:

- (a) parent signature; and
  - (b) written notice that the parent may obtain written information concerning:
    - (i) why the test, treatment, survey, analysis, or evaluation is being administered;
    - (ii) when the test, treatment, survey, analysis, or evaluation will be administered (the date of administration must be at least two (2) weeks from the date of parent notice);
-

- (iii) where the test, treatment, survey, analysis, or evaluation will be administered;
- (iv) who will administer the test, treatment, survey, analysis, or evaluation and who will have access to the information gathered;
- (v) what information is being sought and how it will be collected (i.e., parents must be notified of their right to examine test questions and materials, research proposals and methodologies, etc.);
- (vi) address and phone number of a School employee to whom parents may direct inquiries or concerns (principal, teacher, administrator, etc.).

A general consent used to approve admission to school or involvement in special education, remedial education, or a school activity does not constitute written consent for these purposes.

#### Duration of Parental Authorization

Unless otherwise agreed to by a student's parent or guardian and the person requesting written consent, the authorization is valid only for the activity for which it was granted; or until the parent withdraws consent, during the course of the activity, by submitting a written withdrawal of authorization to the school Principal.

#### Waiver of Parental Notice Period

A parent may waive the 2-week notice period by signing and returning a written waiver to the School.

#### Well-Being of a Student

If a School employee or agent believes that a situation exists that presents a serious threat to the well-being of a student, that employee or agent shall notify the student's parent or guardian without delay. If, however, the matter has been reported to the Division of Child and Family Services (DCFS), it is the responsibility of DCFS to notify the student's parent or guardian.

#### Risk of Suicide

If a school employee or agent believes a student is at risk of attempting suicide, physical self-harm, or harming others, the school employee or agent may intervene and ask a student questions regarding the student's suicidal thoughts, physically self-harming behavior, or thoughts of harming others for the purposes of: (i) referring the student to appropriate prevention services; and (ii) informing the student's parent or legal guardian.

#### **Student Education Records Management**

Parents/guardians have the right to inspect and review all of their student's education

---

records maintained by the School. If the education records of a student contain information on more than one student, the parent/guardian may inspect and review or be informed of only the specific information about their student.

- The School will grant a request by a parent/guardian for access to the education records of their child within a reasonable period of time, but in no case more than forty-five (45) days after the request has been made.

Parents/guardians may challenge and request the School to amend any portion of their student's education record that is inaccurate, misleading or in violation of the privacy rights of the student.

- The School shall consider the request and decide whether to amend the records within a reasonable amount of time. If the Principal decides not to amend the record as requested, the Principal shall inform the parent/guardian of the decision and of their right to a hearing.
- Upon request of a parent or guardian, the School shall provide an opportunity for a hearing to challenge the content of the student's education records on the grounds that the information contained in the education records is inaccurate, misleading, or in violation of the privacy rights of the student.
- Such hearing shall be informal and shall be conducted by an individual who does not have a direct interest in the outcome of the hearing.
- If, as result of the hearing, the School decides that the challenged information is inaccurate or misleading, the record should be amended accordingly and the parent/guardian informed in writing.
- If, as result of the hearing, the School decides that the challenged information is not inaccurate or misleading, it shall inform the parent/guardian of their right to place a statement in the record, commenting on the challenged information in the record, or stating why they disagree with the decision. Any such document must remain with the contested part of the record for as long as the record is maintained, and shall be disclosed whenever the portion of the record to which the statement relates is disclosed.

The School may not disclose information related to education records without prior parental consent, except as provided by law. Such exceptions include, but are not limited to disclosures:

- To school officials who have a legitimate educational interest;
  - To a person or company with whom the School has contracted to perform a special task;
  - To other schools that have requested the records 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;
-

- To individuals who have obtained court orders or subpoenas;
- To individuals who need to know in cases of health and safety emergencies;
- To officials in the juvenile justice system;
- In connection with audit and evaluation of federally or state supported education programs;
- To the Immigration and Naturalization Service (INS) for foreign students attending school under a visa; or
- 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.

The School may disclose directory information for appropriate reasons if it has given parents annual notice of their right to request that their student's directory information not be released by the School.

- The following information relating to students may be declared directory information from time to time:
  - (a) name, address, e-mail address, and telephone number;
  - (b) date and place of birth;
  - (c) major field of study;
  - (d) participation in officially recognized activities and sports;
  - (e) weight and height of members of athletic teams;
  - (f) dates of attendance;
  - (g) degrees and awards received;
  - (h) most recent previous education agency or institution attended; and
  - (i) photograph
- The School shall not release directory information to any individual or organization for commercial use.

The School shall give full rights to student education records to either parent (or guardian), unless the School has been provided with evidence that there is a court order or other legally binding instrument relating to matters such as divorce, separation, or custody that specifically revokes these rights.

### Confidentiality of Student Information

The School and all employees, volunteers, third party contractors, or other agents of the School shall protect the privacy of the student and the student's family through compliance with the protections established under state and federal law.

The School will provide appropriate training to employees regarding the confidentiality of student performance data and personally identifiable student information.

### Data Collection and Storage Procedures

The School will ensure that school enrollment verification data, student performance data, and personally identifiable student information are collected, maintained and transmitted in a secure manner and consistent with sound data collection and storage procedures.

#### Access to Information

Access to confidential student information will be limited to individuals with a legitimate educational interest in the data. The Principal/Director will determine which individuals have a legitimate educational interest in having access to particular data. In general, this will include the Principal/Director, other administrative personnel such as an assistant administrator or counselor, members of the School's front office staff, members of the School's special education staff (in accordance with special education regulations regarding school records), teachers (for students in their classes), and third parties with which the School has contracted to perform special tasks for the School. The School will ensure that all individuals who have access to student information will understand how, where and when they can access this data and will commit to fulfill their obligations to protect the confidentiality of the information.

#### Physical Protection

Any physical documents containing confidential student information will be stored in a secured, locked location. Access to the storage location will be determined by the Principal.

#### Technological Protection

The School will ensure that appropriate technological protections are in place, as described below, whenever the School gathers, transmits, or stores confidential information electronically.

The School currently uses Aspire as its Student Information System. This is the primary location in which the School will store electronic data. This program provides a secure location for the maintenance and transmission of confidential student information. In the event the School decides to use a Student Information System other than Aspire, the School will ensure that the system is approved by USOE and is adequately secure.

The School uses an online registration system for the registration and enrollment of all new students entering the school and for the declaration of current students for re-enrollment. This system is used to run lotteries when applications to the School exceed available openings. The School uses the system to gather student information to enter into the School's Student Information System. This system has been designed with security features that satisfy industry standards. The School will ensure that the system is updated over time to maintain adequate security.

All confidential student information that is stored electronically will be in a location that is password protected. Such data will not be stored on local device drives or on removable data storage media.

The School will ensure that its network, including servers and wireless access components, employs industry standard security measures.

---

School personnel will not share log in information for any system in which confidential student information is stored unless authorized by the Principal.

Confidential student information will only be transmitted through secure means such as Movelt and will not be transmitted via e-mail in an unencrypted format.

#### Personnel Responsibilities

School personnel are responsible for entering student data into the School's Student Information System. This includes information obtained through the School's online registration system and other data gathered throughout the course of the school year. School personnel also manage the maintenance and reporting of records and data required by governmental entities.

The Principal will ensure that School personnel will periodically obtain professional training to ensure that they perform their responsibilities properly and that they comply with all requirements associated with protecting and maintaining the confidentiality of student records and data. This training may include topics such as appropriate and inappropriate access and use of data; who may access data and for what purposes; asking questions when access decisions need to be made; handling problems when misunderstandings arise; data collection procedures and expectations; protecting data during collection, use and storage; key aspects of data security.

#### Third Party Access to Confidential Information

The School's Educational Services Provider, Academica West, will have access to the personally identifiable student data and school enrollment verification data collected and maintained by the School in connection with legitimate educational purposes of the School.

#### Data Breach

The School will notify the parent or guardian of a student if there is a release of the student's personally identifiable student data due to a security breach.

---

# **Free and Reduced Price Policy Certification of Acceptance Submission**

The purpose of the Hazard Materials Procedures is to minimize the exposure and

This policy is effective when it has been signed by an authorized Local  
Education Authority representative and upon State Agency approval.

Wallace Stegner Academy (Local Education Agency or governing body) responsible for administration of one or more schools referred to as the School Food Authority (SFA), has entered into an agreement to participate in the National School Breakfast Program, National School Lunch Program, and/or Special Milk Program and accepts responsibility for providing free and reduced price meals and/or free milk to eligible children in the schools under its jurisdiction.

The SFA assures the Utah State Board of Education-Child Nutrition Programs it will uniformly implement the following policy with respect to determining the eligibility of children for free and reduced price meals in each school building under its jurisdiction participating in the programs mentioned above. Program participation is captured on the site information sheet in CNPweb.

In fulfilling its responsibilities, the LEA agrees to the following:

- A. Primary Free and Reduced Price Eligibility Contact
    - a. The LEA will update the sponsor information sheet in CNPweb with the primary contact designated to make free and reduced price eligibility determinations.
    - b. The determining official will make free and reduced price eligibility determinations using the criteria outlined by USDA regulations, policy and the current year Eligibility Guidance for School Meals guidance.
  - B. Nondiscrimination
    - a. That there will be no physical segregation of, or any other discrimination against, any child because of his/her inability to pay the full price of the meal or milk [7 CFR 245.8].
    - b. LEAs selling competitive foods during a meal service are encouraged to include in the description of how the cafeteria and meal service prevents overt identification of the children receiving free and reduced price meals or free milk.
    - c. The names of children eligible to receive free or reduced price meals or free milk shall not be published, posted, or announced in any manner, and there shall be no overt identification of any such children by use of special tokens or tickets, or by any other means.
    - d. Further assurance is given that children eligible for free or reduced price meals or free milk shall not be required to:
      - i. Work for their meals or milk.
      - ii. Use a separate lunchroom.
      - iii. Go through a separate serving line.
-

- iv. Enter the lunchroom through a separate entrance.
      - v. Eat meals or drink milk at a different time.
      - vi. Eat a meal different from the meal sold to children paying the full price for the same meal or drink milk different from that sold to children paying the full price.
    - e. That in the operation of Child Nutrition Programs, no child shall be discriminated against because of his or her race, sex, age, color, disability, national origin, or reprisal or retaliation for prior civil rights activity in any program or activity conducted or funded by USDA (7 CFR 210 and 7 CFR 245) [7 CFR 15.1].
    - f. The State agency and LEA will ensure there are no barriers for participation in Child Nutrition Programs for Limited English Proficient (LEP) families and the State agency and LEA is required to communicate with parents and guardians in a language they can understand throughout the certification and verification processes.
  - C. Income Eligibility Guidelines (IEGs)
    - a. The LEA certifies the current school year Income Eligibility Guidelines (IEGs) are used to determine free, reduced or paid meal benefits. .
  - D. Public Notification
    - a. Near the beginning of each school year, a public *Media Release* will be distributed statewide by the Utah State Board of Education on behalf of all current National School Breakfast and/or National School Lunch Program sponsors.
    - b. LEAs entering into an agreement after the statewide public release will provide a public media release to the local newspaper, local unemployment office and any major employers contemplating large layoffs in the areas from which the school draws attendance [7 CFR 245.5].
  - E. Free and Reduced Price Meal Applications
    - a. The LEA may use the USDA or Utah State Board of Education *Free and Reduced Price Application* and letter templates.
    - b. The LEA will submit a copy of current year templates if the USDA or Utah State Board of Education Free and Reduced Price templates are not used [7 CFR 245.10(b)]. The state agency will review the forms and templates prior to the LEA sending to households.
  - F. Informing Households
    - i. To inform families about the availability of free and reduced price meals or free milk, the LEA will distribute *Information Letters to Households* of children attending the school [7 CFR 245.5(a)(1)]. CNPs. The information letter must be sent to households before children begin attending school.
      - 1. The information letters must include information as outlined in 7 CFR 245.5(a) including: Income Eligibility Guidelines, instructions on how to apply, general application information,
-

an explanation of assistance programs (SNAP, FDPIR, FEP) household eligibility, an explanation of Other Source Categorically Eligibility, an explanation of eligibility determinations, an explanation of the carryover policy and the full USDA Nondiscrimination Statement.

2. The letters may be distributed by the postal service, e-mailed to the parent or guardian, or included in information packets provided to students.
    - ii. The LEA understands information letters may not be sent to households at the end of the school year for the subsequent school year.
    - iii. The LEA does not accept and process applications before the federally defined school year, which begins on July 1 (year-round schools, however, may distribute the letters in June).
    - iv. The LEA enrolling new students after the start of the school year are provided an *Information Letter to Households, Free and Reduced Price Application*, and materials when they enroll.
  - b. Direct Certification
    - i. Direct certification allows LEAs to establish student eligibility using participating data from another approved program eliminating the need for an application from the household.
      1. During the duration of the USDA FNS Medicaid Demonstration project, the LEA will directly certify students identified as eligible for free or reduced price meals through Medicaid. The LEA will track and report Medicaid direct certification information by free and reduced categories as part of the demonstration project.
    - ii. The LEA ensures all households receive either a *Direct Certification Notice of Eligibility* of their child's approval or, for those not directly certified, an application for free and reduced price meal benefits [7 CFR 245.6].
    - iii. At a minimum, the LEA will utilize CNPweb direct certification matching system to identify exact and potential match students. Students may be directly approved based on their participation in a USDA/state approved assistance program.
    - iv. The CNPweb direct certification matches will occur a minimum of the first, third and sixth operating month of the school year.
  - c. Other Source Categorically Eligible
    - i. The LEA will provide an explanation to households with children who are categorically eligible under *Other Source Categorically Eligible Programs* to contact the school for assistance in receiving benefits and indicate the source of their status on the application.
-

- ii. Other Source Categorical Eligibility of a child does not convey eligibility to other children in the household.
  - 1. Homeless/Migrant/Runaway Children
    - a. The SFA will work with the migrant coordinator, homeless liaison or runaway provider to obtain a list or free and reduced price meal application for children determined to meet the established criteria for homeless, migrant or runaway. The list must include a child's name, effective date of eligibility determination, be dated and signed by the coordinator, liaison or provider. These children are directly certified for free meals for the school year.
  - 2. Foster Children
    - a. The LEA will notify households a *foster child* is categorically eligible for free meals and may be included as a member of the foster family if the foster family chooses to also apply for benefits for other children and an explanation that including children in foster care as household members can help other children in the household qualify for free or reduced price meals. If the foster family is not eligible for free or reduced price meal benefits, this does not prevent a foster child from receiving free meal benefits.
  - 3. Head Start or Eligible Pre-Kindergarten Program
    - a. Federal Head Start and any State-funded pre-kindergarten program that use eligibility criteria that are identical or more stringent than Federal Head Start [7 CFR 245.2].
    - b. A complete application will document the child's status with the Head Start or eligible pre-kindergarten program officials. Information must include children's names, indication of child's categorical eligibility status and signature of adult household member.
    - c. Eligibility of all Head Start enrollees through documentation provided by the Head Start program may include:
      - i. an approved Head Start application,
      - ii. a statement of Head Start enrollment, or
      - iii. a list of participants from a Head Start official.

G. Prevent Overt Identification

- a. The LEA will establish a procedure to collect money which prevents over identification.
-

- b. Point of service meal counting procedures will prevent overt identification of children receiving free or reduced priced meals, milk or a la carte foods (competitive foods). Payment collection methods are identified on the site information sheet in CNPweb.
- c. The LEA will take steps to prevent disclosure of confidential free and reduced price eligibility information as required under 7 CFR 245.6(f-k).

H. Hearing Procedures

- a. The LEA assures adherence to the hearing procedures outlined in the most current Eligibility Manual for School Meals and regulations (7 CFR 210 and 7 CFR 245.7).
- b. The hearing official may not be the same person as the reviewing and/or the verification official.

I. Verification of Applications

- a. Verification procedures and reporting will be in accordance with program regulations [7 CFR 245.6a]. All verification efforts must be completed no later than November 15<sup>th</sup> annually. The verification reports are entered and certified by the SFA no later than November 20<sup>th</sup> annually in CNPweb.

J. Recordkeeping

- a. Program records documenting program benefits and meal counts are preserved for a minimum period of three years plus the current year, or three years plus the current year after a closed audit, and shall be made available for audits or program reviews.
- b. Maintain a file of the following records to which they pertain:
  - i. Public media release identifying where the information was distributed;
  - ii. All eligibility determinations obtained through the Direct Certification Matching Process;
  - iii. All applications and documents to support homeless, migrant, head start, runaway;
  - iv. Records of all appeals
  - v. All notifications of eligibility determinations, including denial letters;
  - vi. Records of all verification efforts and resulting eligibility changes.

*Adam Gerlach*

LEA Authorized Signature	Co-Director
Adam Gerlach	8/2/2018
LEA Signee (Type or Print)	Date

State Agency Signature	Title	Date
------------------------	-------	------

**State Agency:**  Information updated in CNPweb  Final copy in permanent agreement file

□ Signed copy sent to LEA

## **Hazardous Materials Procedures**

The purpose of the Hazard Materials Procedures is to minimize the exposure and accident potential from the use, storage and mixing of chemicals. OSHA requires a Hazard Communication Plan if there are any chemicals that pose a health or physical hazard located on the property or in any building that is occupied by employees of the school. Our plan includes the following elements:

1. We will only store chemicals with like properties together on any shelf or in any container in our building.
2. We will identify all chemicals on the property and make an inventory of all chemicals that pose a health or physical threat to our employees.
3. The chemical inventory sheet and an MSDS for each chemical will be composed and stored in all places where chemicals are mixed, stored, or used or in the office of our main building and everyone on the property shall be informed of its location and how to find the pertinent information on the sheets for any emergency or for normal preventive measures for each chemical.
4. Training for the safe use of each chemical shall be done before any employee uses the chemical for the first time and again every time a new chemical is purchased for the same purpose.
5. The chemical inventory shall be updated at least once each year, and the old chemical inventory shall be archived to verify which chemicals were used and for how long they were used at the school.
6. No employee will be allowed to bring any chemical onto the school property without the permission of the Principal, the custodian and any other person exposed to the chemical.
7. All new chemicals must have their MSDS sheets reviewed by the safety committee before they can be used at the school.

Anyone who fails to abide by this rule could be held personally liable for any injury or damage from the chemical to students, employees or anyone entering the building.

## Hiring Procedures

The School will adhere to the following procedures in connection with hiring any employee of the School.

All offers of employment must be approved by the Principal prior to extending the offer.

A signed employment application will be obtained prior to extending an offer of employment.

References will be checked prior to extending an offer of employment.

The School will ensure that documentation of employment applications and reference checks will be maintained for an appropriate length of time.

Written employment agreements will be obtained for all employees. All employment agreements must be signed by the Principal. Employees must complete all required new hire paperwork, including but not limited to Form I-9, within the required time frame.

Background checks will be completed in accordance with Utah law and School policy prior to any employee commencing work.

New employees will be oriented with respect to School policies and procedures.

New employees will be provided a copy of the School's Employee Handbook, and documentation of this will be maintained.

# Home and Hospital Request Forms

## Parent's Request for Home and Hospital

Student \_\_\_\_\_  
Last First MI

Address \_\_\_\_\_  
Street City State Zip

Grade \_\_\_\_\_ Last day of school attendance \_\_\_\_\_

Parent Contact Info: \_\_\_\_\_  
Last First MI

Home Phone \_\_\_\_\_ Work/Cell Phone \_\_\_\_\_

Reason for Request \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

I authorize an official with Wallace Stegner Academy to consult, when necessary, with the physician attending my son/daughter to confirm the diagnosis and/or clarify the medical notations. I am also aware that Home and Hospital is for temporary situations (60-day maximum) and should not be used on a long-term basis.

\_\_\_\_\_  
Parent Signature

## Physician's Request for Home and Hospital

This is to certify that the above named student was examined by me on \_\_\_\_\_.

Is patient recommended to be home?

- Yes  
 No

I will be responsible for continuing of treatment or supervision during the time he/she is out of school?

- Yes  
 No

Diagnosis: \_\_\_\_\_.

Is this contagious?

- Yes  
 No

If yes, list of precautions to be taken by staff to minimize risk of transmission of disease:

---

---

If home and hospital is recommended, please state the reason:

---

---

Treatment length: \_\_\_\_\_

Treating Medical Professional's Name: \_\_\_\_\_  
(please print)

Phone: \_\_\_\_\_ Fax: \_\_\_\_\_

Signature: \_\_\_\_\_

## Human Sexuality Instruction Procedures

These administrative procedures are established pursuant to the Human Sexuality Instruction Policy adopted by the School's Board of Directors.

In accordance with state law, all human sexuality instruction or instructional programs will comply with the requirements of Utah Code § 53A-13-101 and -301 through -302 and Utah Admin Code R277-474. Specifically, the School will:

- teach sexual abstinence before marriage and fidelity after marriage as methods for preventing certain communicable diseases;
- teach personal skills that encourage individual choice of abstinence and fidelity;
- obtain prior parental consent before any human sexuality instruction or instructional program.

The Principal will establish a curriculum materials review committee composed of parents, schools employees, and others selected by the Principal. The committee will have at least as many parents as school employees. The School's Board of Directors will approve the membership of the committee annually.

The curriculum materials review committee will review and make recommendations to the School's Board of Directors regarding instructional materials to be used by the School in connection with human sexuality instruction. Program materials and guest speakers supporting instruction on these topics must also be reviewed and approved by the curriculum materials review committee.

Instructional materials used by the School in connection with human sexuality instruction must be approved by the School's Board of Directors in an open meeting. These materials will comply with the requirements of applicable law and will be available for parents to review for a reasonable period of time prior to consideration for adoption by the Board of Directors.

The following topics may not be taught in the School:

- The intricacies of intercourse, sexual stimulation or erotic behavior;
- The advocacy of encouragement of the use of contraceptive methods or devices;  
or
- The advocacy of sexual activity outside of marriage.

The School will comply with the Utah Family Educational Rights and Privacy Act, Utah Code § 53A-13-301, through -302 and obtain parental consent prior to any human sexuality instruction or instructional program. At no time will a student be in the classroom during any human sexuality instruction or instructional program unless an approval form signed by the student's parent/guardian is on file.

Instructors may not intentionally elicit comments or questions about matters subject to parental consent requirements. Additionally, instructors' responses to questions spontaneously raised by students must be brief, factual, objective and in harmony with content requirements of this policy and state law. Responses must also be age appropriate and limited in scope to that reasonably necessary under the circumstances.

The School will ensure that instructors with any responsibility for any aspect of human sexuality instruction will receive proper training. Additionally, the School will ensure that such instructors are familiar with requirements of the Utah Family Educational Rights and Privacy Act.

# Information Technology Systems Security Plan

## 1. PURPOSE

The primary purpose of this Information Technology Systems Security Plan is to establish security measures that will help Wallace Stegner 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.

# Meal Charge and Alternate Meal Procedures

## Wallace Stegner Academy Meal Charge Procedures

### A. Purpose and Background

(1) The National School Lunch Program (“NSLP”) and National School Breakfast Program (“NSBP”) are programs that WSA offers.

(2) The purpose of this procedure is to explain how WSA will notify parents/guardians about: money owed for student meals; the School’s procedures for providing meals if students’ accounts are delinquent; and to assure and remind parents and School employees that students will never be confronted or embarrassed about money owed for school meals.

### B. Information Provided to Parents

(1) Prior to or at the beginning of each school year, parents shall receive information from WSA regarding:

- (a) School meals;
- (b) Prices for the meals;
- (c) How parents may provide payment for meals; and
- (d) The NSLP and NSBP and how students may qualify for reduced-price or free meals under the programs, including an application for free or reduced-price meals.

(2) WSA shall provide the information described above as follows:

- (a) Information will be provided to WSA students and families regarding school meals, prices, payments and how to qualify and apply for free and reduced school meals through the following means: School newsletter at the beginning of the school year, printed and available at Back-to-School Night, and given to all students on the 1st day of school. It will also be printed and available in the School office beginning at Back-to-School Night and throughout the school year.
- (b) During Back-to-School Night WSA will provide applications for free/reduced-price meals to parents, both by providing printed copies and by providing access to a computer to fill out an electronic application online. WSA will also have a computer set up during parent teacher conferences and during regular business hours (as needed) for the purpose of filling out an electronic application online. The application is accepted year round and available in a variety of languages at: <https://www.fns.usda.gov/school-meals/translated-applications>. The School will provide paper applications for parents who do not have access to online forms. The School will also add links to its website for applications for free or reduced-price meals.

(3) Prior to or at the beginning of each school year, and upon a student transferring to the School during the school year, WSA will provide to the parent of each student a written copy of this procedure by including it in the registration packet and having copies available at the front office year round. This procedure will also be posted on the School's website at [www.wsacharter.org](http://www.wsacharter.org), under the Breakfast and Lunch tab section. Students, parents, and the School community were involved in developing these communication procedures.

(4) If a parent or family qualifies for one of the following programs SNAP, FEP, FRRIP, or Medicaid and has not received a qualification for free or reduced-price lunch letter before school starts, the parent should contact the School's front office. Parents should also contact the School's front office for questions about the NSLP or NSBP or for assistance with applying for free or reduced-price school meals.

### **C. Payments and School Verification**

(1) WSA must verify at some point in each student's meal service that the meal is reimbursable or non-reimbursable.

(2) WSA will credit meal payments from parents to the student's account within 48 hours, working with banking holidays and schedules. This assures all funds are accurately applied to meal accounts as soon as possible before students are selecting school meals.

(3) If a student/family qualifies for free meals, no payments are due.

(4) If a family qualifies for reduced-price meals, the School will charge no more than \$.30 for breakfast and \$.40 for lunch.

(5) Parent payment options for student meals may include:

(a) Parents may make online payments, using debit or credit cards, for one or all of their students, allocating the funds to individual student's accounts. There are additional fees for making payments by credit card through the School website. To make an online payment through the School website, parents must click on the Breakfast and Lunch tab and go to the link for instant payments. A third party handles all online payments; and

(b) Parents may make payments to the School by mail or hand delivery. Payments should clearly indicate the account to which the funds should be credited (student's name and amount, if several students attend the School). WSA also accepts payments by check and/or cash at the School.

### **D. Identification of Delinquent Accounts**

(1) WSA will identify accounts weekly and notify parents by email of negative balances. WSA may ask students to take notifications addressed to the parent home with them;

however, the School will not tell students to “remind” their parents to send money to the School. It is the parents’ responsibility to pay the student’s account. Asking students to remind parents is inappropriate.

(2) The School may use any of the following options (or other reasonable options) for student meals if a student’s meal account is inadequate:

- (a) Student may bring a sack meal from home; and
- (b) School may continue to provide an alternate meal to students and notify parents that the School will use collection efforts to pay for meals. The School shall maintain documentation of parent notice.

(3) If a student’s account is delinquent, the School may offer the student an alternate meal and charge the students account \$1.00 for that meal, instead of serving a full meal at the full price.

### **E. Delinquent Balances and Other Procedures**

(1) There is a -\$15.00 limit on charge accounts. After the limit we may provide an alternate meal and charge the student’s account \$1.00.

(2) Lunch accounts with an unpaid balance from a previous school year will not be allowed to charge meals. Students will be allowed to bring a full cash payment for their meal that day, but no charging will be allowed until all past due funds are paid in full.

(3) We will notify parents of students with delinquent balances in their school lunch accounts by such methods as:

- (a) Weekly e-mail on accounts from negative \$.01-\$19.99;
- (b) Phone Call from negative \$20.00 to \$35.00; and
- (c) Account turned over to collections negative \$35.00 and above.

(4) If no payment is received, the account will be turned over to a collection agency when the student’s account becomes negative \$35. (No federal funds may be used for the collection of funds). WSA will notify parents at least twice annually concerning their procedures for the collection of past-due accounts.

(5) WSA may complete an application for free/reduced-price meals on behalf of the parents, if School personnel have knowledge of the parents’ financial circumstances and parents give permission. The School will notify parents that an application has been completed on their behalf (“Eligibility Manual for School Meals,” July, 2015, pg. 45).

(6) If a student repeatedly has no money in the student’s school lunch account and no student meals are provided from home, School officials will consider the circumstances in the home (e.g., potential abuse or neglect, homelessness, etc.) and may contact the WSA social worker and/or Child Protective Services.

(7) WSA will use collection agencies to collect on delinquent accounts.

## **F. Faculty/Staff/Patrons**

(1) As a Child Nutrition Program, our responsibility is to the students of WSA. We love when parents, grandparents, older siblings, Aunt, Uncles, Family Members, Teachers, Aides, Administration and any visitors come to have lunch with our students and in our School. Parents and guests may purchase lunch using their student's accounts if there are funds in the account to cover the meals. All non-student meals are \$3.50. When any other account besides student accounts hit a zero balance (\$0.00), meals may be denied until funds or a receipt for funds being deposited into the account that day is presented to the point of sale person.

(2) The School will annually provide a copy of this procedure to all School personnel who are responsible for or involved in:

- (a) Collecting payment for meals at the time of meal service;
- (b) Notifying parents of delinquent accounts;
- (c) Collection efforts for delinquent accounts;
- (d) Distributing this procedure and other information about the NSLP and NSBP;  
and
- (e) Enforcing any aspect of this procedure.

## **G. Review of Procedures**

(1) The School will review this procedure annually and revise it as the School deems necessary.

# Religion and Education Procedures

## Implementation

1. At least once a year, the Principal will review with teachers and staff the School's Religion and Education Policy (the "Policy"), the associated procedures, and related statutes and regulations. This review will stress the Board's expectation that School personnel will recognize, protect, and accommodate religious freedom and individual rights of conscience in the operation of the School, while fostering mutual understanding and respect for all individuals and beliefs.
2. The Board 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 notified annually of their rights under the Policy, state law, and state administrative rules. The notice will contain at least the following information:
  - a. A copy of the Policy, rules, and related statutes and regulations regarding religion in the curriculum will be available upon request in the school office;
  - b. A secondary school student, or parent or legal guardian of any student, may make a complaint to the Principal that a portion of the curriculum, a School activity, or the conduct of a School employee violates state or federal law insofar as it "promotes or disparages a particular religious, denominational, sectarian, agnostic, or atheistic belief or viewpoint." (Utah Code §53A-13-101.1(4));
  - c. A secondary school student, or parent or legal guardian of any student, may make a request to the Principal for a waiver of participation in any portion of the curriculum or a School activity, which the student, parent, or legal guardian believes is an infringement of the student's right of conscience or the exercise of religious freedom in any of the following ways:
    - i. It requires the affirmation or denial of a religious belief or practice, or right of conscience.
    - ii. It requires participation in a practice forbidden by a religious belief or practice, or right of conscience.
    - iii. It bars participation in a practice required by a religious belief or practice, or right of conscience.
  - d. Pursuant to Utah State Administrative Rules (R277-105-5.B), a claimed infringement must rise to a level of belief that the requested conduct violates a superior

duty which is more than personal preference in order to, justifying waiver of participation.

4. The Principal will discuss annually with the Board any requests for accommodation, or complaints about religion in the curriculum, made within the last year in order to determine how the School can more effectively recognize, protect, and accommodate religious freedom and individual rights of conscience in the operation of the School. In discussing these matters with the Board, the Principal will take care to protect the privacy rights of those who made complaints or requests. The Principal will also submit the written record of each complaint received and any decisions made regarding such complaints to the Board President.

### **Requests for Waiver of Participation**

In general, and within the bounds of law, such requests by secondary students, or parents or legal guardians of any students, to be excused or refrain from participating in activities, discussions, and assignments they feel would violate their rights of conscience or religious freedom will be granted routinely and without penalty.

Any student, parent, or legal guardian who desires a waiver of participation or substitution of another activity as provided in Utah State Board Administrative Rules (R277-105-5) will put that request in writing and direct it to the Principal.

Once a student, parent, or legal guardian has requested a waiver of participation, the student will not be compelled to participate in any curriculum or activity pending resolution of the request, unless the Principal has determined that requiring the participation of that particular student in that particular activity is the least restrictive means necessary to achieve a specifically identified educational objective in furtherance of a compelling governmental interest. (R277-105-5.F)

The principal, student, the student's parent or legal guardian, and the teacher or employee responsible for the program in question will meet to discuss the request. The Principal will arrive at a decision, swiftly and in a manner consistent with state law, whether to waive participation, alter the curriculum or activity, substitute another activity, or require the student's participation. The Principal will encourage the student and student's parent or guardian to suggest a reasonable alternative. In making a decision, the Principal will give proper consideration to any suggestions made by the student and the student's parent or guardian.

The Principal will keep a written record of every request for a waiver of participation or substitution of activity based on religious freedom or right of conscience and any decisions made regarding each request.

## **Complaints Alleging Violation of Law**

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

The Principal, 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 Principal 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 Principal will give a written decision as soon as practical under the circumstances.

The Principal will keep a written record of every complaint and any decisions made regarding each complaint.

The Board President will personally, or by a committee of his or her choosing, evaluate the curriculum or activity in question. If the Board President is concerned that any curriculum or activity may violate state or federal law, he or she may determine whether the educational objectives could be achieved by less restrictive means and may request that the Principal alter or substitute another curriculum or activity.

## **Appeals Process**

A student, parent, or legal guardian who is dissatisfied with a Principal's decision regarding either requests for waiver of participation or 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 principal and may modify the Principal'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 Principal. 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 President will keep a written record of every appeal and any decisions made regarding each appeal.

The decision of the Board President will be final.

## **Safety Procedures**

The Principal will establish a safety committee that is comprised of the Principal or another administrator, a front office employee, a teacher, and at least one parent selected by the Principal. These committee members may add others to the committee as they see fit. For instance, the committee may wish to include police officers, firefighters, or paramedics or other individuals with safety expertise that may benefit the School. The committee will meet at least three (3) times each year to discuss matters related to the safety of the School for students, employees, and visitors, including but not limited to the School's emergency response plan, building access procedures, School procedures for things such as carpooling and parking lot safety, School activities, the condition of the School's building(s) and equipment, the causes of recent student and employee accidents, the existence of conditions in and around the School that could pose a safety risk. The committee may make recommendations regarding feasible ways to reduce any risks identified.

The Principal will ensure that the School building and equipment are inspected at least annually in order to identify any potentially unsafe conditions. The School will maintain a written record of the inspections and corrective actions for any unsafe conditions that were identified.

All accidents that result or that may be expected to result in any injury and/or require any medical treatment will be documented.

Any incidents that may result in claims against the School or the School's insurance must be promptly reported to the Principal. The Principal will ensure that a report is made to the School's insurance carrier as necessary.

Any property damage incidents such as vandalism, theft, or break in will be reported to the police.

## **Snow and Ice Removal Procedures**

The School contracts with a company for snow removal services on a yearly basis. The service agreement extends to cover all expected months of snowfall. When snowfall accumulations are expected to reach or exceed two inches, the removal company is responsible for clearing all walks, parking areas, entrances and exits, and hardscape playground areas. In addition to pushing snow, salt and/or ice melt is distributed throughout the parking lot and on all walkways. The contracted company is instructed to schedule the School's snow removal as close as possible to the times of arrival and departure of students and staff as these times are the heaviest for pedestrian traffic. During winter break, the snow removal company is responsible for clearing snow and distributing salt and ice melt.

When accumulations are less than two inches, shovels, other snow removal equipment and ice melt are stored at the School. The Principal or designated employee(s) monitor the conditions of the campus's sidewalks and walkways, is responsible to remove the snow from walkways and distribute ice melt on walks. If snow melts and results in ice patches, it is the Principal's decision as to how to proceed. The Principal may call the contracted company for additional salt and ice melt, or more commonly, may distribute or direct an employee to distribute ice melt on walkways. Effort is made to address ice patches and snow prior to student and staff arrival and throughout the day to minimize slipping hazards.

## Student Data Disclosure Statement

Wallace Stegner Academy (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.

Student data collected by the School includes data defined as “necessary student data” and “optional student data” in Utah Code Ann. § 53A-1-1402(17)-(18). The School collects student data primarily through registration, but it also collects additional student data during the school year. The necessary and optional student data collected by the School is listed in the School’s Data Governance Plan, which is (or will soon be) available on the School’s website. The School does not collect a student’s social security number or, except as required in Utah Code Ann. § 78A-6-112, criminal record.

The School strives to not share a student’s personally identifiable student data unless the sharing is in accordance with the Utah Student Data Protection Act, Utah Family Educational Rights and Privacy Act, and the federal Family Educational Rights and Privacy Act. Except as allowed by law, the School will not share, externally, personally identifiable student data from a cumulative record without a data authorization. Examples of where the law allows the School to share personally identifiable student data without a data authorization include sharing such data with a school official, an authorized caseworker or other representative of the Department of Human Services, or a person to whom the School has outsourced certain services or functions that School employees would typically perform. Student data collected by the School and shared with outside parties is set forth in the School’s Metadata Dictionary, which is (or will soon be) available on the School’s website.

The School takes many measures to protect its student data. Student data stored digitally by the School is stored on computers and systems that are secured, maintained, and supported by qualified IT service providers. Confidential personally identifiable student data in print form is stored in secured, locked areas in the School.

A student’s rights under Utah’s Student Data Protection Act include:

- Each student owns his or her personally identifiable student data and may download, export, transfer, save, or maintain their student data, including a document;
- A student’s parent or guardian, or an adult student, has the right to be notified by the School if there is a release of the student’s personally identifiable student data due to a security breach;
- Except where otherwise provided by law, a student is entitled to have his or her student data expunged by the School if the student is at least 23 years old and requests that the School expunge his or her student data; and
- A student is entitled to receive a student data disclosure statement from the

School.

**The collection, use, and sharing of student data has both benefits and risks. Parents and students should learn about these benefits and risks and make choices regarding student data accordingly.**

## **Student Injury Reporting Procedures**

All student injuries, including but not limited to cuts, abrasions, bruises, and sprains, occurring at school or during school-sponsored activities must be reported to the office on a Student Injury Report Form by the individual with the most firsthand knowledge of the incident. Depending on the nature of the injury, the student's teacher, the Principal, or a member of the office staff will notify the student's parent(s) of the injury. Unless the severity of the injury requires emergency medical assistance for the student, school personnel will consult with the student's parent(s) regarding medical treatment for the injury.

## Volunteer Procedures

“Volunteer” means any person who donates service without pay or other compensation except expenses actually and reasonably incurred as approved by the School.

School volunteers are an important part of the educational team and can make a significant difference in the lives of students. The School’s volunteer program can provide a rich resource of community members who can assist faculty and staff in diverse ways.

### Responsibilities and Expectations

Volunteers shall perform volunteer services under the supervision of an assigned school employee and shall have the approval of the Principal to perform such volunteer services.

Volunteers are expected to follow the direction of the school employee to whom they have been assigned and to conform to all applicable laws, rules, and policies.

In the course of volunteering for the School, volunteers may be asked to deal with confidential information. The School expects that volunteers shall keep such information in the strictest confidence.

In accordance with School policy regarding Religion and Education, volunteers must maintain strict neutrality regarding religion while performing volunteer services for the School.

Failure to follow the direction of a supervisor or to follow applicable laws, rules and policies may preclude the volunteer from continuing to serve the School. Serving as a volunteer in the educational setting is not an entitlement, and the School is not required to utilize volunteer services. The opportunity to volunteer may be denied or terminated by the Principal for any reason or no reason, including but not limited to situations where services are no longer needed or where the presence of the volunteer may be disruptive to the educational environment.

### Appointing and Managing Volunteers

The School will adhere to the following guidelines in the selection and management of volunteers.

1. Assess the needs, special qualifications and requirements for any positions for which volunteers are being considered in order to determine whether it will be appropriate to have volunteers in those positions.
2. Develop basic job descriptions for individual jobs or classes of jobs to be performed by volunteers. Just as with paid employees, all volunteers should be

covered by written job descriptions. Ask questions such as the following and reflect those details in the written job description:

- a. Will the volunteer be alone with students?
  - b. How closely will the volunteer be supervised?
  - c. Will the volunteer operate his/her own vehicle while performing School business?
  - d. Will the volunteer have access to money or other valuable equipment?
  - e. Will the volunteer supervise other volunteers or staff?
  - f. Will the volunteer be involved in any activities that require special qualifications?
3. Based on the foregoing analysis, develop a process to ensure that qualified individuals are selected to fill volunteer positions.
  4. Make sure that volunteers are aware of the policies and procedures that apply to their activities so that they know what may and may not be done. Have volunteers sign to verify that they have received the applicable policies and procedures.
  5. Assign a staff member as the supervisor and primary contact person for each volunteer.
  6. Before placing volunteers in any job, ensure that both they and their supervisor are properly trained in the rules that govern the activities and the functions of the job the volunteer will be performing. Make sure the volunteer and the supervisor understand the job description for the position. Document the training that was provided.
  7. Create an individual file for each volunteer as appropriate to keep track of hours spent and activities performed.
  8. Evaluate the volunteer's performance and provide volunteers with feedback regarding their performance. Document the evaluation and feedback provided.
  9. Correct improper volunteer behavior and discipline volunteers as appropriate. Document such actions.
  10. Volunteers engaged to provide ongoing services to the School must sign an Agreement for Voluntary Services.

### Background Checks

Pursuant to Utah Code § 53A-1a-512.5(1), volunteers who will be given significant unsupervised access to a student in connection with the volunteer's assignment (including but not limited to transporting students in a vehicle) must receive a criminal background check as a condition for appointment to that position.

Volunteers must be given written notice that the background check has been requested.

The School may only consider convictions that are job-related in deciding whether to appoint a volunteer.

The School will pay the cost of the background check.

The volunteer must be given the opportunity to respond to any information received through the background check. The School's administration will consider such information prior to deciding whether to appoint or retain the volunteer.

#### Immunity from Liability and Workers' Compensation

Under Utah state law, volunteers performing volunteer services under the general supervision of a school employee are immune from liability with respect to any decisions or actions, other than in connection with the operation of a motor vehicle, taken during the course of those services, unless it is established that such decisions or actions were grossly negligent, not made in good faith, or were made maliciously.

An approved volunteer is considered a government employee for purposes of receiving workers' compensation medical benefits, which shall be the exclusive remedy for all injuries and occupational diseases as provided by law.