



**Official Procedure
of
Ogden Preparatory Academy**

8. Parents and Community

8.04.PRC.1 FERPA Administrative Procedures

Page 1 of 5

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, antisocial, 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:
 - a. why the test, treatment, survey, analysis, or evaluation will be administered;

- b. the date of administration must be at least two (2) weeks from the date of parent notice;
- c. where the test, treatment, survey, analysis, or evaluation will be administered;
- d. who will administer the test, treatment, survey, analysis, or evaluation and who will have access to the information gathered;
- e. 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.);
- f. 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 parents 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 that 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 purpose of: (i) referring the student to appropriate prevention services; and (ii) informing the student’s parent or legal guardian.

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/Director.

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/Director.

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/Director 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 Providers, 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.

Document History

Approved:

Revised: