Confidentiality of Student Records Policy

This policy replaces all previous Confidentiality of Student Records policies.

INTRODUCTION

Pursuant to the Family Education Rights and Privacy Act (FERPA) and other applicable state and federal laws, confidentiality of Aspire student records is a priority. Fiscal agents are responsible for ensuring confidentiality of records. Please communicate this policy to all Aspire-paid and volunteer staff.

GENERAL

A. FERPA requires that, with certain exceptions, education agencies obtain written consent prior to the disclosure of personally identifiable information (PII) from a student record. However, FERPA allows education agencies to disclose appropriately- designated "directory information" without written consent unless the student has advised the agency to the contrary in accordance with agency procedures. Aspire programs must comply with the procedures set by their fiscal agents regarding notifying students and, if applicable, parents annually of their rights under FERPA.

For additional Information about FERPA visit:
FERPA Training
Model Notice for Directory Information

B. Appropriate measures must be taken to ensure confidential student records are protected from loss, theft or other compromise. Student records may be transported to and from approved data entry sites only, and their confidentiality and safety must be ensured at all times. **Student records may not be taken to a public location** (e.g. staff member's home, other non-Aspire work location).

ELECTRONIC RECORDS

C. All local Aspire programs are responsible for ensuring that data entry is completed only by authorized Aspire staff. Authorized staff must complete a Personal Confidentiality Statement (PCS) Form, maintain their own login information, and keep the information secure. The completed PCS form must be received in the Aspire office by June 30 each year to receive or continue access in the new fiscal year. The individual requesting access to LACES (data management system) on the PCS form may not be the same person who authorizes access. For example, an Aspire director may sign for data entry staff, but the director may not sign for his/her own access. The Aspire director's supervisor or a higher-level individual in the organization, such as the CFO, CEO, or college president, must approve the director's access.

All new users in the LACES system must first complete the Introductory LACES training, which includes security and usage requirements.

Users who have not accessed the system for 120 consecutive days shall have their account deactivated by the local agency's system administrator—they will need to complete the PCS process again to resume access. Reactivation is not automatic and will be dependent on the user's prior access history and job role. Access granted is at the discretion of the State Aspire Office.

Each local agency is limited to one system administrator who is responsible for creating and determining the access levels of new and existing LACES accounts. The number of accounts local programs may create is at their discretion. Careful consideration should be used when deciding who has access to higher-level system functionality and limited to job duties that necessitate access. ODHE reserves the right to terminate access if it is determined that user accounts have been misused.

D. Secure transmission methods, as defined by the local agency, with NIST (National Institute of Standards of Technology) and state standards in mind, must be used when transmitting student data electronically—this includes intra- and inter-agency email communication containing student PII. Sending PII via email should be avoided if possible. If unavoidable, the most sensitive PII (SSN, for example) should still never be shared via email.

E. Cloud computing, the delivery of various services through the use of internet/web-based software, is not prohibited by FERPA. Local agencies should use reasonable methods to ensure the security of their information technology solutions. Additional information can be found in the USDOE's Cloud Computing FAQ documentation.

F. ODHE does not assume responsibility for sanctions imposed by the USDOE stemming from student privacy violations. Grant funding may not be used to cover any resulting fines.

RELEASE OF INFORMATION/REVOCATION OF RELEASE

The Ohio Department of Higher Education (ODHE) requires that all Aspire programs provide the Release of Information Form (RIF) and/or the Revocation of Release of Information Form (R-RIF) to every student during orientation. The required form may be downloaded from ohiohighered.org/aspire/reference, under the heading **Required Documents**. The release of student information initiates the state data match process in which all Aspire programs are required to participate. Local program and state accountability for employment and HSE completion is determined through the data match process and supplemented by follow-up survey completion.

The Student Registration Form must indicate whether the student has signed the RIF or R-RIF, and the signed form must be kept on file with the local Aspire program. If the box on the Student Registration Form has not been checked indicating the student signed the RIF, the student will be excluded from all data match or information sharing between agencies designated on the form. The RIFs are valid until revoked by the student or the minor student's parent/guardian.

The RIF requires the student's signature (and parent/guardian's signature if the student is under 18) in order to authorize ODHE to release his/her educational records, including the student's name; Social Security Number; student ID number; and date of birth, to the agencies listed on the RIF.

Agency use of these records is limited to, and in connection with, the audit and evaluation of federally-supported education programs, or in connection with the enforcement of federal legal requirements, that relate to such programs. FERPA does not require a signature for the postsecondary education data match, but the student should be informed that his/her record will be matched with ODHE data to determine entry into or completion of postsecondary education.

Additionally, the RIF authorizes the release of educational records between Aspire programs when the student opts to receive educational services through differing Aspire providers.

USE OF SOCIAL SECURITY NUMBERS AND DATA MATCH REQUIREMENTS

Aspire programs must also request the Social Security Number of all students during orientation which should be entered into the data management system and will be used to facilitate the state data match. If a student does not have a Social Security Number or is unwilling to disclose it, the student is still eligible to enroll in a local Aspire program. The student will, in this case, be excluded from data matches which require this information, but will not be exempt from follow-up calculations.

Local Aspire programs must continue to complete follow-up surveys to supplement data matches. The survey form may be downloaded from ohiohighered.org/aspire/reference, under the heading **Surveys.** A list of students surveyed and the survey results must be kept on file in the local program office.

This is a policy established by the Ohio Department of Higher Education's state Aspire office. Questions concerning this policy should be directed to your regional Aspire Program Manager. LiteracyPro Systems provides support in the use of LACES, not interpreting or enforcing policies set by this office.