



Arizona Department of Education

GUIDELINE:	Data Extract Request and Release Guidelines	Guideline No:	IT XX-YY-0906171500
Scope:	ADE	Effective:	
Expiration:	This guideline is to be reviewed, and either revised or allowed to renew unchanged by:		
	Key Contact(s): R. Rachkofski, M. Cruz		

I. PURPOSE

The purpose of this guideline is to establish the authority and procedures for releasing data extracts of sensitive and confidential student detail information or aggregated data created from this data to associated schools, school districts and charter schools, and to such agencies or entities that may have a legitimate need to view them, and the legal right to do so.

II. GUIDELINE

It is the Arizona Department of Education's (ADE) operating principle to safeguard sensitive and/or confidential information pertaining to a student's identity, and the associated data related to the identified student when it is extracted from ADE databases and physically or electronically delivered to the appropriate school, local education agency (LEA), charter school entity, or other duly authorized agency. Legal mandates require that data be submitted by educational entities to ADE. Those data or subsets of data are to be made available to those entities, or to any legally authorized agency, upon request. The chief administrator or a designated senior official of the educational entity should make a formal request. When other agencies, such as the Attorney General or Auditor General have a need and the right to possess any student-level data collected by ADE, both the process of requesting and the delivery of data should be properly documented for public inspection and auditing purposes to ensure that the transfer of information followed proscribed procedures.

III. PROCEDURE SUMMARY

Note: For a more detailed description of the Data Request Workflow please refer to Appendix A.

A. The LEA or other agency requiring a data extract notifies ADE's Data Management Team of the specific data request and its intended use. This should be done by means of a letter on the LEA's or agency's letterhead, signed by the agency head, chief administrator, or a senior official. An alternate method of request can be via e-mail with a recognizable and verifiable e-mail return address. The requester will be sent the Request/Release form attached below. Pending the completion and return of the form along with the identity verification of the requester (i.e. photocopy of driver's license or employee badge), the request will be vetted by the Data Management team and the result of this process will be to authorize, reject (with cause), or further clarify the requirements with the requesting agent.

B. If the request is rejected, a Data Management representative will notify the requester and explain the reasons for that decision. Adjustments to the request may be made and resubmitted if appropriate.

C. If the request is authorized either directly or after needed clarifications have been made, an estimate of the delivery time will be made. The complexity of the request, workload, and staffing levels may all be contributing factors to this estimate.

D. The Data Management analyst will generate the extract and load it into a package on an encrypted Web server. A notification (with full instructions) will be sent to the recipient. The recipient will navigate to the site and click a link and enter the username and password previously assigned. Using this SSL (Secure Socket Layer) technology, the file will then be decrypted for the recipient.

E. For later reference, quality control inspection, and audit purposes, the original request, the extraction script, and the result set will be archived.

Arizona Department of Education

RELEASE/RECEIPT FOR DATA EXTRACT OR RELEASE

Directions: Please complete all portions of this form. The completed form must be retained as a permanent record.

Section A: Requestor Information

Date of Request: June 13, 2012

Name and Title: David Stuit, Managing Partner, Basis Policy Research

Address: Basis Policy Research, 206 Grandville Ave., Suite 370, Grand Rapids, MI 49503

Email Address: dastuit@basispolicyresearch.com

Phone Number: 616-821-5811 **Fax Number:** 1-888-628-0516

Section B: Please check what type of data user you are:

Internal ADE Employee External User

Section C: Check the following fields that apply regarding the data request

Data will be published Data resides on ADE Public Website New Report Request
 Data is reported to FEDS Data Warehouse User (Section E) Other
 Data is for Promotional Purpose Authorized to receive Educational Data ADE collects the Data
 Data is Student Level (Section G&I) Data is Confidential (Section G&I) Raw Data

Section D: Precise Description of the Data Requested, and its Intended Use:

Full description of data request (include attachment if necessary):

1. Data with student level AIMS test scores in grades 3 to 8 and 10 in Math and Reading, student level AIMS Science test scores in grades 4, 8 and 10, and student level AIMS Writing test scores in grades 5 to 7 and 10. The dataset should include all tested students in Arizona public schools. Student test results should be expressed in scale scores. Each student observation should have a unique student ID that is linkable to other data. If available, we would like to have the estimate standard errors of measurement (SEMs) associated with student test scores included in the test file. We would also like to have other variables included in the AIMS file, such as district ID, district name, school ID, school name, and homeroom teacher/teacher of record (if available).
2. Data with student level SAT10 test scores in grades 2 and 9 in math, reading and language arts. Similar as the AIMS test files, the SAT 10 test files should include all 2nd and 9th grade students in Arizona public schools. Test scores should be expressed in scale scores. If available, SEMs should be included in the test file. We would like to have studentIDs, district IDs, school IDs, district names and school names included in the file.
3. Other student level data on student background/demographic characteristics: (1) Student Background: student birth date, student name, race, gender, eligibility for federal free reduced price lunch program, migrant status, homeless status, and mother education; (2) Special Education/Program: special education status, gifted education status, ELL, LEP, FEP; (3) Mobility: student new to the district, new to the school, and transfer school within the year etc. Other variables might be student ID, school ID, school name, district ID, and district name. The student IDs should be linkable to the test files and other student level data.
4. Student level enrollment data. Student enrollment data include a student's record of the entry/withdrawal date in/out each school within a school year. This will be used to build the school-student link for each student. A student may have multiple records in this data, each representing the school where the student enrolled within a school year. Student IDs and school IDs should be linkable with other data files.
5. Student level attendance data (if available). For every school in which a student enrolled in the school year, the attendance data provides attendance, tardy, and absence information. If a student enrolled in multiple schools within a school year, he/she should have multiple records. We are not sure what attendance data

1. Be responsible for the information obtained, use it appropriately, and only for authorized purposes;
2. Only use individual records or anything that could generate personally identifiable information for the validation of queries/programming;
3. Destroy student level records that have been provided from the Data Warehouse student information pursuant to a formal agreement within time limitations defined in the agreement and provide certification to the Data Management staff that such records have been destroyed;
4. Provide to the Data Management team, prior to publication/release, any documents generated as a result of using data received from the Data Warehouse, for review and verification that the stated purpose has been honored;
5. Understand that deliberate or accidental misuse of information may result in one or more of the following: loss of access, disciplinary action, prosecution under the scope of all applicable federal and state laws;
6. Ensure the data obtained is stored and transmitted securely and not available or disclosed to unauthorized parties; and
7. Encrypt the data on mobile computing devices containing any data retrieved from the Data Warehouse that pertains to an individual's level, status, or identity (student or staff).

Users must not:

1. Use the results of information provided by or generated from AEDW data to determine the identity of any student or employee;
2. Allow any unauthorized use of information provided by or generated from the AEDW data;
3. Share any data with any other individual(s) that has the potential to be personally identifiable; and
4. Publish reports with cell sizes of less than 10. (Reports must mask these cells so that personal identities cannot be extrapolated.)
5. Before any data is published it must be submitted to the Data Warehouse Group for approval

Notice of Limitations

The Data Warehouse is best used for doing longitudinal analysis. It acquires its data from the **SAIS Student Details** system, the **AIMS** subsystem, and other ADE managed data repositories. The accuracy of the data in the Data Warehouse is as good as the accuracy of the data in these source systems. The submitted data are screened for adherence to prescribed formats and for logical consistency. Error reports are sent to the submitting schools for the correction of these types of errors only.

1. The data in the SAIS Student Details system are submitted by the LEAs. The AZELLA (language assessments) data prior to 2009 were also submitted by the LEAs. From FY 2009 forward AZELLA data are being submitted by the testing vendor.
2. The data in the AIMS system are submitted by the testing vendor.

Note: The source systems are not formally audited, either by the Auditor General, or by the ADE Auditor. Further, ADE cannot attest to the veracity of these self reported or vendor reported data for their evidentiary value.

The Data Warehouse is not intended and should not be used for the determination or analysis of state funding. The Data Warehouse does not apply the strict business rules used for state equalization funding.

Section F: ADE Employee Who Is Authorizing the Release of Data:

The undersigned ADE employee (a) understands that the information described above may include sensitive, personal, or confidential data, (b) affirms that she or he is duly authorized to release ADE information, and (c) hereby authorizes its release to the entity/person below.

(ADE Employee Signature)

(Date)

(ADE Employee Printed Name)

(ADE Department or Unit)

Section G: Person Who is Requesting the Data:

The undersigned acknowledges receipt of information as described above, understands that it may include sensitive or personal or confidential information, and accepts responsibility for safeguarding it as appropriate. The undersigned is aware of the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. §1232g; 34 CFR Part 99), understands that it is a federal law that protects the privacy of student educational records, and recognizes that there are severe penalties for its violation. Also, contained in the Arizona Title 15-Education; Section 15-537; <http://www.azleg.gov/ArizonaRevisedStatutes.asp?Title=15> is the adherence of state laws governing school employees confidential information.



(Signature)

David Stuit

(Printed Name)

June 13, 2012

(Date)

Basis Policy Research working on behalf of
Maricopa County Educational Service Agency

(Requesting Agency, Department or Educational Entity)

Section H: ADE Employee Who Is Actually Releasing the Data:

The undersigned ADE employee affirms (1) that the person receiving the data extract described above was properly identified by photo credential as checked below, and (2) that ADE has received proper authorization from the responsible local education agency to release its data, as checked below. Proper written authorization is a letter of release on the requesting agency's letterhead signed (by the agency head, chief administrator, or a senior official), or other appropriate formal document including identifiable and verifiable e-mail.

1) I identified the person who is receiving the information by the following photo credential:

driver's license employee badge other (describe): _____

2) I have attached a photocopy of the photo credential:

3) The responsible LEA/agency authorized release of this information by:

written authorization other (describe): _____

(ADE Employee Signature)

(Date)

(ADE Employee Printed Name)

(ADE Department or Unit)

Section I: FERPA

The purpose of FERPA is two-fold: to assure that parents and eligible students can access the student's education records, and to protect their right to privacy by limiting the transferability of their education records without their consent. 120 Cong. Rec. 39862. As such, FERPA is not an open records statute or part of an open records system. The only parties who have a right to obtain access to education records under FERPA are parents and eligible students. Journalists, researchers, and other members of the public have no right under FERPA to gain access to education records for school accountability or other matters of public interest, including misconduct by those running for public office. Nonetheless, as explained in the preamble to the NPRM, 73 FR 15584-15585, we believe that the regulatory standard for defining and removing personally identifiable information from education records establishes an appropriate balance that facilitates school accountability and educational research while preserving the statutory privacy protections in FERPA. The simple removal of nominal or direct identifiers, such as name and SSN (or other ID number), does not necessarily avoid the release of personally identifiable information. Other information, such as address, date and place of birth, race, ethnicity, gender, physical description, disability, activities and accomplishments, disciplinary actions, and so forth, can indirectly identify someone depending on the combination of factors and level of detail released.