

CW 35512

DSA No. K1933

DATA SHARING AGREEMENT
BETWEEN
STATE OF WASHINGTON
OFFICE OF FINANCIAL MANAGEMENT
AND
THE UNIVERSITY OF TEXAS AT AUSTIN
CHARLES A DANA CENTER

This Agreement is made and entered into by and between the **OFFICE OF FINANCIAL MANAGEMENT**, hereinafter referred to as "OFM", and CHARLES A DANA CENTER, hereinafter referred to as "DANA CENTER", pursuant to the authority granted in Chapters 39.34 and 43.41 of the Revised Code of Washington, relevant federal statutes, and related regulations.

AGENCY CONTACTS: OFFICE OF FINANCIAL MANAGEMENT

Agreement Administrator:
Name: Jim Schmidt
Title: ERDC Director
Division: Forecasting
Address: PO Box 43124 Olympia 98504-3124
Phone: 360-902-0595
E-mail: jim.schmidt@ofm.wa.gov

ORGANIZATION CONTACTS: CHARLES A DANA CENTER

Agreement Administrator:
Name: Jennifer Dorsey
Title: Senior Evaluation Associate
Address: 1616 Guadalupe Suite 3206 Austin, TX
Phone: 512-232-4728
E-mail: dorseyjen@austin.utexas.edu

1. PURPOSE OF THE DATA SHARING AGREEMENT

The purpose of this Data Sharing Agreement (DSA) is to provide DANA CENTER with an individual-level data set of education outcomes linked to survey data provided by the DANA CENTER in order:

1. Assess the degree to which these programs change learning mindsets and strategies over the course of these programs
2. Examine the predictive validity of the learning mindsets and strategies survey constructs.

2. DEFINITIONS

"Agreement" means this Data Sharing Agreement, including all documents attached or incorporated by reference.

“Data Encryption” refers to ciphers, algorithms or other encoding mechanisms that will encode data to protect its confidentiality. Data encryption can be required during data transmission or data storage depending on the level of protection required for this data.

“Data Storage” refers to the state data is in when at rest. Data shall be stored on secured environments.

“Data Transmission” refers to the methods and technologies to be used to move a copy of the data between systems, networks, and/or workstations.

“Disclosure” means to permit access to or release, transfer, or other communication of personally identifiable information contained in education or employment records by any means including oral, written, or electronic means, to any party except the party identified or the party that provided or created the record (34 CFR 99.3).

“OFM Data” means data provided by OFM, whether that data originated in OFM or in another entity.

“Personally Identifiable Information” means information that can be used to distinguish or trace an individual’s identity, such as their name, Social Security Number, student number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc. Personally Identifiable Information also includes other information that, alone or in combination, would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty. In the case of employment data, this means information which reveals the name or any identifying particular about any individual or any past or present employer or employing unit, or which could foreseeably be combined with other publicly available information to reveal any such particulars (20 CFR 603.4).

3. PERIOD OF AGREEMENT

This Agreement shall begin on April 17, 2017 or date of execution, whichever is later, and end on December 31, 2020 unless terminated sooner or extended as provided herein.

4. DESCRIPTION OF DATA TO BE SHARED

For survey participants provided by the DANA CENTER, OFM shall provide the following data: Research ID, school and district, Academic Youth Development (AYD) and Intensified Algebra (IA) flags at the school level. Student enrollment in AYD or IA classes or Tumwater High School, student characteristics (gender, race/ethnicity), student program participation (FRPL, ELL, SpEd), number of days attended, number of unexcused absences, disciplinary data (if available), statewide math assessment (raw score, scale score, level for Smarter Balance and Algebra EOC), math course taking patterns (algebra by 8th grade, algebra in 9th grade, algebra grade, algebra credit y/n) and math courses taken 8th through 12th grade (course name, grade, credit/no credit).

5. DATA TRANSMISSION

To ensure data is encrypted during data transmission, all data transfers to/from DANA CENTER shall be transmitted using the Consolidated Technology Services FTP Service with login and hardened password security. OFM shall create an account for the data requestor if an account does not already exist.

6. DATA SECURITY

All data provided by OFM shall be stored on a secure environment with access limited to the least number of staff needed to complete the purpose of this Agreement.

a. Protection of Data

DANA CENTER agrees to store data on one or more of the following media and protect the data as described:

- 1) Workstation Hard disk drives. Data stored on local workstation hard disks. Access to the data shall be restricted to authorized users by requiring logon to the local workstation using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. If the workstation is located in an unsecured physical location the hard drive must be encrypted to protect OFM data in the event the device is stolen.
- 2) Network server disks. Data stored on hard disks mounted on network servers and made available through shared folders. Access to the data shall be restricted to authorized users through the use of access control lists which will grant access only after the authorized user has authenticated to the network using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers shall be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism. Backup copies for DR purposes shall be encrypted if recorded to removable media.
- 3) Optical discs (e.g. CDs, DVDs, Blu-Rays) in local workstation optical disc drives. Data provided by OFM on optical discs which shall be used in local workstation optical disc drives and which shall not be transported out of a secure area. When not in use for the Agreement purpose, such discs are required to be locked in a drawer, cabinet or other container to which only authorized users have the key, combination or mechanism required to access the contents of the container. Workstations which access OFM data on optical discs shall be located in an area which is accessible only to authorized individuals, with access controlled through use of a key, card key, combination lock, or comparable mechanism.
- 4) Optical discs (e.g. CDs, DVDs, Blu-Rays) in drives or jukeboxes attached to servers. Data provided by OFM on optical discs shall be attached to network servers and which shall not be transported out of a secure area. Access to data on these discs shall be restricted to authorized users through the use of access control lists which will grant access only after the authorized user has authenticated to the network using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on discs attached to such servers shall be located in an area which is accessible only to authorized individuals, with access controlled through use of a key, card key, combination lock, or comparable mechanism.
- 5) Paper documents. Any paper records shall be protected by storing the records in a secure area, which is only accessible to authorized individuals. When not in use, such records shall be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

- 6) Access via remote terminal/workstation over the State Governmental Network (SGN). Data accessed and used interactively over the SGN. Access to the data shall be controlled by OFM staff who will issue authentication credentials (e.g. a unique user ID and complex password) to authorized individuals. DANA CENTER shall notify the OFM Agreement Administrator immediately whenever an authorized person in possession of such credentials is terminated or otherwise leaves, and whenever a user's duties change such that the user no longer requires access to perform work for this Agreement.
- 7) Access via remote terminal/workstation over the Public Internet only through Secure Access Washington. Data accessed and used interactively over the SGN. Access to the data shall be controlled by OFM staff who shall issue authentication credentials (e.g. a unique user ID and complex password) to authorized individuals. DANA CENTER shall notify the OFM Agreement Administrator immediately whenever an authorized person in possession of such credentials is terminated or otherwise leaves, and whenever a user's duties change such that the user no longer requires access to perform work for this Agreement.
- 8) Data storage on portable devices or media.
 - a) OFM data shall not be stored by DANA CENTER on portable devices or media unless specifically authorized within this Agreement. If so authorized, the data shall be given the following protections:
 - i. Encrypt the data with a key length of at least 128 bits
 - ii. Control access to devices with a unique user ID and password or stronger authentication method such as a physical token or biometrics.
 - iii. Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes.
 - iv. Physically protect the portable device(s) and/or media by:
 - Keeping them in locked storage when not in use;
 - Using check-in/check-out procedures when they are shared; and
 - Taking frequent inventories.
 - b) When being transported outside of a secure area, portable devices and media with confidential OFM data shall be under the physical control of DANA CENTER staff with authorization to access the data.
 - c) Portable devices include, but are not limited to; handhelds/PDAs, Ultramobile PCs, flash memory devices (e.g. USB flash drives, personal media players), portable hard disks, and laptop/notebook computers.

- d) Portable media includes, but is not limited to; optical media (e.g. CDs, DVDs, Blu-Rays), magnetic media (e.g. floppy disks, tape, Zip or Jaz disks), or flash media (e.g. CompactFlash, SD, MMC).

b. Safeguards Against Unauthorized Access and Re-disclosure

DANA CENTER shall exercise due care to protect all Personally Identifiable data from unauthorized physical and electronic access. Both parties shall establish and implement the following minimum physical, electronic and managerial safeguards for maintaining the confidentiality of information provided by either party pursuant to this Agreement:

- 1) Access to the information provided by OFM shall be restricted to only those authorized staff, officials, and agents of the parties who need it to perform their official duties in the performance of the work requiring access to the information as detailed in the Purpose of this Agreement.
- 2) DANA CENTER shall store the information in an area that is safe from access by unauthorized persons during duty hours as well as non-duty hours or when not in use.
- 3) Unless specifically authorized in this Agreement, DANA CENTER shall not store any confidential or sensitive OFM data on portable electronic devices or media, including, but not limited to laptops, handhelds/PDAs, Ultramobile PCs, flash memory devices, floppy discs, optical discs (CDs/DVDs), and portable hard disks.
- 4) DANA CENTER shall protect the information in a manner that prevents unauthorized persons from retrieving the information by means of computer, remote terminal or other means.
- 5) DANA CENTER shall take precautions to ensure that only authorized personnel and agents are given access to on-line files containing confidential or sensitive data.
- 6) DANA CENTER shall instruct all individuals with access to the Personally Identifiable Information regarding the confidential nature of the information, the requirements of Use of Data and Safeguards Against Unauthorized Access and Re-Disclosure clauses of this Agreement, and the sanctions specified in federal and state laws against unauthorized disclosure of information covered by this Agreement.
- 7) DANA CENTER shall take due care and take reasonable precautions to protect OFM's data from unauthorized physical and electronic access. Both parties will strive to meet or exceed the requirements of the State of Washington's policies and standards for data security and access controls to ensure the confidentiality, availability, and integrity of all data accessed.

c. Data Segregation

- 1) OFM data shall be segregated or otherwise distinguishable from non-OFM data. This is to ensure that when no longer needed by the DANA CENTER, all OFM data can be identified for return or destruction. It also aids in determining whether OFM data has or may have been compromised in the event of a security breach.
- 2) OFM data shall be kept on media (e.g. hard disk, optical disc, tape, etc.) which shall contain no non-OFM data. Or,

- 3) OFM data shall be stored in a logical container on electronic media, such as a partition or folder dedicated to OFM data. Or,
- 4) OFM data shall be stored in a database, which will contain no non-OFM data. Or,
- 5) OFM data shall be stored within a database and will be distinguishable from non-OFM data by the value of a specific field or fields within database records. Or,
- 6) When stored as physical paper documents, OFM data shall be physically segregated from non-OFM data in a drawer, folder, or other container.
- 7) When it is not feasible or practical to segregate OFM data from non-OFM data, then both the OFM data and the non-OFM data with which it is commingled shall be protected as described in this Agreement.

If DANA CENTER or its agents detect a compromise or potential compromise in the IT security for this data such that personal information may have been accessed or disclosed without proper authorization, DANA CENTER shall give notice to OFM within one (1) business day of discovering the compromise or potential compromise. DANA CENTER shall take corrective action as soon as practicable to eliminate the cause of the breach and shall be responsible for ensuring that appropriate notice is made to those individuals whose personal information may have been improperly accessed or disclosed.

7. DATA CONFIDENTIALITY

DANA CENTER acknowledges the personal or confidential nature of the information and agrees that their staff and contractors with access shall comply with all laws, regulations, and policies that apply to protection of the confidentiality of the data. If data provided under this Agreement is to be shared with a subcontractor, the contract with the subcontractor shall include all of the data security provisions within this Agreement and within any amendments, attachments, or exhibits within this Agreement. If the Contractor cannot protect the data as articulated within this Agreement, then the Contract with the subcontractor must be submitted to the OFM Agreement Administrator specified for this Agreement for review and approval.

a. Non-Disclosure of Data

- 1) Individuals shall access data gained by reason of this Agreement only for the purpose of this Agreement. Each individual (staff and their contractors) with data access shall read and sign Exhibit A, Statement of Confidentiality and Non-Disclosure, prior to access to the data. Copies of the signed forms shall be sent to the OFM Agreement Administrator identified on Page 1 of this Agreement, who will distribute them to the other educational agencies as appropriate.
- 2) OFM may at its discretion disqualify at any time any person authorized access to confidential information by or pursuant to this Agreement. Notice of disqualification shall be in writing and shall terminate a disqualified person's access to any information provided by OFM pursuant to this Agreement immediately upon delivery of notice to DANA CENTER. Disqualification of one or more persons by OFM does not affect other persons authorized by or pursuant to this Agreement.

b. Penalties for Unauthorized Disclosure of Information

In the event DANA CENTER fails to comply with any terms of this Agreement, OFM shall have the right to take such action as it deems appropriate. The exercise of remedies pursuant to this paragraph shall be in addition to all sanctions provided by law, and to legal remedies available to parties injured by unauthorized disclosure.

8. USE OF DATA

- a. Data provided by OFM shall remain the property of OFM and shall be returned to OFM or destroyed when the work for which the information was required has been completed.
- b. This Agreement does not constitute a release of the data for DANA CENTER's discretionary use, but may be accessed only to carry out the responsibilities specified herein. Any ad hoc analyses or other use of the data, not specified in this Agreement, is not permitted without the prior written agreement of OFM. DANA CENTER shall not disclose, transfer, or sell any such information to any party, except as provided by law. DANA CENTER shall maintain the confidentiality of all Personally Identifiable Information and other information gained by reason of this Agreement.
- c. DANA CENTER is not authorized to update or change any OFM data, and any updates or changes shall be cause for immediate termination of this Agreement.
- d. Neither Washington State nor OFM guarantees the accuracy of the data provided. All risk and liabilities of use and misuse of information provided pursuant to this Agreement are understood and assumed by DANA CENTER.
- e. Data provided by OFM cannot be linked with other data or data sets as a way to determine the identity of individuals or employers; the data in any data set shall be used for statistical purposes only. Using OFM data to identify students or employers shall be cause for immediate termination of this Agreement and may prevent data sharing agreements with the organization in the future. If the identity of any student or employer is discovered inadvertently, DANA CENTER shall not use this information and shall advise OFM of any such discovery.
- f. Data provided by OFM cannot be re-disclosed or duplicated unless specifically authorized in this Agreement.
- g. DANA CENTER shall follow applicable federal and state laws protecting student and employment data, and the guidelines specified in the Institute of Education Sciences SLDS Technical Brief 3, Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting (NCES 2011-603 <http://nces.ed.gov/pubs2011/2011603.pdf>) when displaying student information in public reports. Publicly-reported aggregated results will not contain any group of fewer than 10 individuals, and percent ranges should be used, where the greater the uncertainty (smaller number of observations) the greater width of the reporting range.
- h. When displaying employment data, cell sizes should be ample enough so one record does not contain 80% of the wages or hours of a particular reporting cell. Other considerations when using employment

data can be found in ERDC Technical Report 2012-01, Employment Data Handbook located at http://erdc.wa.gov/briefs/pdf/EmploymentDataHandbook_v1.pdf.

- i. DANA CENTER shall include the following excerpts with any public release using OFM data:

“The research presented here utilizes confidential data from the Education Research and Data Center (ERDC), located within the Washington Office of Financial Management (OFM). Committed to accuracy, ERDC’s objective, high-quality data helps shape Washington’s education system. ERDC works collaboratively with educators, policymakers and other partners to provide trustworthy information and analysis. ERDC’s data system is a statewide longitudinal data system that includes de-identified data about people’s preschool, educational, and workforce experiences. The views expressed here are those of the author(s) and do not necessarily represent those of the OFM or other data contributors. Any errors are attributable to the author(s).”

- j. DANA CENTER shall provide draft report(s) to OFM and data contributors at least ten (10) working days prior to any public release of reports and communicate with OFM or data contributors when questions arise regarding data provided.
- k. The requirements in this section shall survive the termination or expiration of this agreement or any subsequent agreement intended to supersede this DSA.

9. DISPOSITION OF DATA

- a. Once this agreement ends, through expiration or termination, DANA CENTER shall dispose of the data received and provide written notification of disposal (See Exhibit B). Failure to do so may prevent data sharing agreements with the organization in the future.
- b. Upon the destruction of OFM data, DANA CENTER shall complete Exhibit B Certification of Data Disposition, and submit it to the OFM Agreement Administrator within fifteen (15) days of the date of disposal.
- c. Acceptable destruction methods for various types of media include:
 - 1) For paper documents containing confidential or sensitive information, a contract with a recycling firm to recycle confidential documents is acceptable, provided the contract ensures that the confidentiality of the data will be protected. Such documents may also be destroyed by on-site shredding, pulping, or incineration.
 - 2) For paper documents containing Confidential Information requiring special handling, recycling is not an option. These documents must be destroyed by on-site shredding, pulping, or incineration.
 - 3) If confidential or sensitive information has been contained on optical discs (e.g. CDs, DVDs, Blu-ray), the data recipient shall either destroy by incineration the disc(s), shredding the discs, or completely deface the readable surface with a coarse abrasive.
 - 4) If confidential or sensitive information has been stored on magnetic tape(s), the data recipient shall destroy the data by degaussing, incinerating or crosscut shredding.

- 5) If data has been stored on server or workstation data hard drives or similar media, the data recipient shall destroy the data by using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data, degaussing sufficiently to ensure that the data cannot be reconstructed, or physically destroying disk(s).
- 6) If data has been stored on removable media (e.g. floppies, USB flash drives, portable hard disks, or similar disks), the data recipient shall destroy the data by using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data, degaussing sufficiently to ensure that the data cannot be reconstructed, or physically destroying disk(s).

10. ON-SITE OVERSIGHT AND RECORDS MAINTENANCE

DANA CENTER agrees that OFM shall have the right, at any time, to monitor, audit and review activities and methods in implementing the Agreement in order to assure compliance therewith, within the limits of DANA CENTER's technical capabilities.

Both parties hereto shall retain all records, books, or documents related to this Agreement for six years, except data destroyed in Section 9. The Office of the State Auditor, federal auditors, and any persons duly authorized by the parties shall have full access to and the right to examine any of these materials during this period.

11. INDEMNIFICATION

To the extent allowed by law, each party to this Agreement shall be responsible for any and all acts and omissions of its own staff; employees, officers, agents and independent contractors. To the extent allowed by law, each party shall furthermore defend and hold harmless the other party from any and all claims, damages, and liability of any kind arising from any act or omission of its own staff, employees, officers, agents, and independent contractors.

12. AMENDMENTS AND ALTERATIONS TO THIS AGREEMENT

With mutual consent, OFM and DANA CENTER may amend this Agreement at any time, provided that the amendment is in writing and signed by authorized staff.

13. ORDER OF PRECEDENCE

In the event of an inconsistency in this Contract, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

- a. Applicable Federal and State laws;
- b. Any other provisions of the Contract whether by reference or otherwise.

14. TERMINATION

a. For Convenience

Either party may terminate this Agreement with thirty (30) days' written notice to the other party's Agreement Administrator named on Page 1. In case of termination, any and all information provided by OFM pursuant to this agreement shall either be immediately returned to OFM or immediately destroyed. Written notification of destruction to OFM is required.

b. For Cause

OFM may terminate this Agreement at any time prior to the date of completion if and when it is determined that DANA CENTER has failed to comply with the conditions of this Agreement. OFM shall promptly notify DANA CENTER in writing of the termination and the reasons for termination, together with the effective date of termination. In case of termination, the data provided by OFM shall be returned to OFM or destroyed on or before the date of termination. Written notification of destruction to OFM is required.

15. SEVERABILITY

The provisions of this Agreement are severable. If any provision of this Agreement is held invalid by any court; that invalidity shall not affect the other provisions of this Agreement and the invalid provision shall be considered modified to conform to the existing law.

16. SIGNATURES

The signatures below indicate agreement between the parties.

OFFICE OF FINANCIAL MANAGEMENT

Bonnie Lindstrom
Signature

Bonnie Lindstrom
Printed Name

Contracts Coordinator
Title

05.16.2017
Date

CHARLES A. DANA CENTER

Linda Shalensky
Signature

Linda Shalensky
Printed Name

Ops Contracts
Title

4/18/2017
Date

EXHIBIT A

STATEMENT OF CONFIDENTIALITY AND NON-DISCLOSURE
between the

State of Washington

OFFICE OF FINANCIAL MANAGEMENT
and the
CHARLES A DANA CENTER

As an employee of DANA CENTER, I have access to information provided by the State of Washington, Office of Financial Management (OFM). This information is confidential, and I understand that I am responsible for maintaining this confidentiality. I understand that the information may be used solely for the purposes of work under DSA No. K1933.

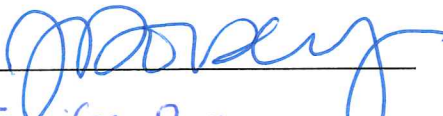
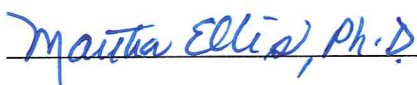
- I have been informed and understand that all information related to this DSA is confidential and may not be disclosed to unauthorized persons. I agree not to divulge, transfer, sell, or otherwise make known to unauthorized persons any information contained in this system.
- I also understand that I am not to access or use this information for my own personal information but only to the extent necessary and for the purpose of performing my assigned duties as an employee of DANA CENTER under this Agreement. I understand that a breach of this confidentiality will be grounds for disciplinary action which may also include termination of my employment and other legal action.
- I agree to abide by all federal and state laws and regulations regarding confidentiality and disclosure of the information related to this DSA.

Employee

I have read and understand the above Notice of Nondisclosure of information.

Supervisor

The employee has been informed of their obligations including any limitations, use or publishing of confidential data.

Signature		
Printed Name	<u>Jennifer Dorsey</u>	<u>Martha Ellis, Ph.D.</u>
Organization	<u>Charles A. Dana Center</u>	<u>Charles A. Dana Center</u>
Job Title	<u>Senior Evaluation Analyst</u>	<u>Interim Director, Higher Education Services</u>
E-mail address	<u>dorseyjen@austin.utexas.edu</u>	<u>mellis@austin.utexas.edu</u>
Date	_____	_____

Please return signed forms to OFM, PO Box 43124, Olympia, WA 98504-3124

DSA No. K1933

EXHIBIT B

Certification of Data Disposition

Date of Disposition _____

___ All copies of any data sets related to DSA No. K1933 have been wiped from data storage systems.

___ All materials and non-wiped computer media containing any data sets related to DSA No. K1933 have been destroyed.

___ All copies of any data sets related to DSA No. K1933 that have not been disposed of in a manner described above, have been returned to the Contractor's Contract Manager listed in this Contract.

The data recipient hereby certifies, by signature below, that the data disposition requirements as provided in DSA No. K1933 Data Disposition section of this Program Agreement have been fulfilled as indicated above.

Signature of Contract Manager _____ Date: _____

Return original to OFM Agreement Administrator indicated on page 1 of this Contract. Retain a copy for your records.