DATA SHARING AGREEMENT
BETWEEN
STATE OF WASHINGTON
OFFICE OF FINANCIAL MANAGEMENT,
OFFICE OF SUPERINTENDENT OF PUBLIC INSTRUCTION,
AND
COMMUNITY COLLEGES OF SPOKANE

This Agreement is made and entered into by and between the **OFFICE OF FINANCIAL MANAGEMENT**, hereinafter referred to as "OFM", and **COMMUNITY COLLEGES OF SPOKANE**, hereinafter referred to as "CCS", 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 43113 Olympia 98504-3113
Phone:	360-902-0595
E-mail:	jim.schmidt@ofm.wa.gov

AGENCY CONTACTS: STATE BOARD OF COMMUNITY AND TECHNICAL COLLEGES

	Agreement Administrator:
Name:	David Prince
Title:	Director, Policy Research
Division:	Educational Services
Address:	PO Box 42495 Olympia 98504-2495
Phone:	360-704-4347
E-mail:	dprince@sbctc.edu

AGENCY CONTACTS: OFFICE OF SUPERINTENDENT OF PUBLIC INSTRUCTION

	Agreement Administrator:
Name:	Debra Came
Title:	Director
Division:	Student Information
Address:	PO Box 47200 Olympia 98504-7200
Phone:	360-725-6356
E-mail:	deb.came@k12.wa.us

ORGANIZATION CONTACTS: COMMUNITY COLLEGES OF SPOKANE

	Agreement Administrator:	Technical Administrator:
Name:	John O'Rourke	Mark Macias
Title:	Grants & Contracts Manager	Managing Director of Institutional Research
Division:		
Address:	PO Box 6000, MS 1006	
Phone:	509-434-5185	509-434-5240
E-mail:	john.orourke@ccs.spokane.edu	mark.macias@ccs.spokane.edu

1. PURPOSE OF THE DATA SHARING AGREEMENT

The purpose of this Data Sharing Agreement (DSA) is to provide CCS identifiable K-12 data for school districts participating in the Student Transitions Information Project (STIP). STIP is a grant-funded, longitudinal, student data tracking project that follows former K-12 students into post-secondary education and the workforce. Analyses will be summarized into reports and provided to the participating school districts. ERDC is being asked to provide this data on behalf of the school districts and OSPI to lessen the burden on the participating school districts. Participating school districts, identified as those having signed data-sharing memorandums of understanding with CCS include those listed in Exhibit C. CCS is responsible for the recruitment of new partners institutions/districts, for the management and maintenance of appropriate DSAs with those partners, and for providing copies of all partner DSAs to the ERDC.

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 March 1, 2015, or date of execution, whichever is later, and end on June 30, 2017, unless terminated sooner or extended as provided herein.

4. DESCRIPTION OF DATA TO BE SHARED

Cohort includes only students who have graduated from a participating school district, one record per student in a tab-delimited text file using definitions in Exhibit D.

5. DATA TRANSMISSION

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

6. DATA SECURITY

All identifiable 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

CCS 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 will 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 will 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 must 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 must 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 will be used in local workstation optical disc drives and which will not be transported out of a secure area. When not in use for the Agreement purpose, such discs must 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 must 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 which will be attached to network servers and which will not be transported out of a secure area. Access to data on these discs will 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 must 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 must be protected by storing the records in a secure area which is only accessible to authorized individuals. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

6) OFM data shall not be stored by CCS on portable devices or media.

b. Safeguards Against Unauthorized Access and Re-disclosure

CCS 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 will 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) CCS will 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, the CCS will 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) CCS will protect the information in a manner that prevents unauthorized persons from retrieving the information by means of computer, remote terminal or other means.

5) CCS shall take precautions to ensure that only authorized personnel and agents are given access to electronic or paper files containing confidential or sensitive data.

6) CCS 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) CCS 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 must be segregated or otherwise distinguishable from non-OFM data. This is to ensure that when no longer needed by the CCS, 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 will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-OFM data. Or,

3) OFM data will be stored in a logical container on electronic media, such as a partition or folder dedicated to OFM data. Or,

4) OFM data will be stored in a database which will contain no non-OFM data. Or,

5) OFM data will 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 will 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 must be protected as described in this Agreement.

If CCS 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, CCS shall give notice to OFM and all partner institutions/districts within one (1) business day of discovering the compromise or potential compromise. CCS shall take corrective action as soon as practicable to eliminate the cause of the breach. Notification to partner institutions/districts will include documentation which can be used by partners to, on behalf of CCS, notify any of their students whose personal information may have been improperly accessed or disclosed. CCS will also have primary responsibility for notifying its own students who might have been affected.

7. DATA CONFIDENTIALITY

CCS 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 must 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 will 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 CCS. 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 CCS 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 will remain the property of OFM and will 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 CCS's discretionary use, but may be accessed only to carry out the responsibilities specified herein and the data-sharing memorandums of understanding for STIP. Any ad hoc analyses or other use of the data, not specified in this Agreement or the data-sharing MOU, is not permitted without the prior written agreement of OFM and the participating school districts. CCS shall not disclose, transfer, or sell any such information to any party, except as provided by law. CCS shall maintain the confidentiality of all Personally Identifiable Information and other information gained by reason of this Agreement.

c. CCS 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 CCS.

e. Data provided by OFM cannot be disclosed or duplicated unless specifically authorized in this Agreement.

f. CCS 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.

g. 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.

h. CCS 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). 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)."

i. Provide draft report 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.

j. 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. Upon termination of the agreement, CCS 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, CCS 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) The data will be stored on servers or Storage Area Network arrays and when needed, the data recipient will destroy the data by the use of this method: a SQL purge of the data, and the data space overwritten. In the case of backup tapes or hard drives, the data will first be deleted and overwritten, then one or both of these processes will be employed: 1) degauss, then incinerate, 2) drill platters, then incinerate. This will ensure that the data cannot be reconstructed.

10. ON-SITE OVERSIGHT AND RECORDS MAINTENANCE

CCS 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 CCS'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

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. 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. DATA BREACH

If CCS detects a breach in the IT security for this data such that Personally Identifiable Information may have been accessed or disclosed without proper authorization, they will give notice to OFM within one (1) business day of discovering the breach, and will take corrective action as soon as practicable to eliminate the cause of the breach. CCS is responsible for providing documentation of the incident to partner institutions/districts which can be used by partners to notify any of their students who might have been affected by the breach. CCS is also responsible for providing notification to any CCS students who records were involved.

13. AMENDMENTS AND ALTERATIONS TO THIS AGREEMENT

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

14. 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.

15. 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 CCS has failed to comply with the conditions of this Agreement. OFM shall promptly notify CCS 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.

16. GOVERNING LAW

This Agreement shall be construed under the laws of the State of Washington. Venue shall be proper in Superior Court in Thurston County, Washington.

17. 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.

18. SIGNATURES

The signatures below indicate agreement between the parties.

OFFICE OF FINANCIAL MANAGEMENT

Bonnie Lindstrom
Signature

Bonnie Lindstrom
Printed Name

Contracts Coordinator
Title

07.14.2015
Date

COMMUNITY COLLEGES OF SPOKANE

John O'Rourke
Signature

John O'Rourke
Printed Name

Grants and Contracts Manager
Title

6-29-15
Date

OFFICE OF SUPERINTENDENT OF PUBLIC INSTRUCTION

Signature

DEB LAME
Printed Name

Director of Student Information
Title

6/18/2015
Date

STATE BOARD FOR COMMUNITY AND TECHNICAL COLLEGES

Signature

David Prince
Printed Name

Director Policy Research
Title

2/2/15
Date

EXHIBIT A

STATEMENT OF CONFIDENTIALITY AND NON-DISCLOSURE

between the

State of Washington

OFFICE OF FINANCIAL MANAGEMENT

and the

COMMUNITY COLLEGES OF SPOKANE

As an employee of CCS, 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. K1177.

- 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 CCS 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.
- I agree to abide by the terms of this confidentiality and non-disclosure agreement during the term defined by this DSA and indefinitely thereafter.

	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	_____	_____
Organization	_____	_____
Job Title	_____	_____
E-mail address	_____	_____
Date	_____	_____

Please return signed forms to OFM, PO Box 43113, Olympia, WA 98504-3113

EXHIBIT B

Certification of Data Disposition

Date of Disposition _____

___ All copies of any data sets related to DSA No. K1177 have been wiped from data storage systems.

___ All materials and non-wiped computer media containing any data sets related to DSA No. K1177 have been destroyed.

___ All copies of any data sets related to DSA No. K1177 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. K1177 Data Disposition section of this Program Agreement have been fulfilled as indicated above.

Signature of Contract Manager_____ Date: _____

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

DSA No. K1177

EXHIBIT C

Last Revised: 10/2/2014

K12 District Partners (n=42)

District Name	District ID
Central Valley School District	32356
Chewelah School District	33036
Colton School District	38306
Columbia (Stevens) School District	33206
Creston School District	22073
Curlew School District	10050
Cusick School District	26059
Davenport School District	22207
Deer Park School District	32414
East Valley School District (Spokane)	32361
Eastmont School District	09206
Goldendale School District	20404
Grandview School District	39200
Granger School District	39204
Inchelium School District	10070
Kittitas School District	19403
LaCrosse School District	38126
Liberty School District	32362
Lind School District	01158
Mabton School District	39120
Mary Walker School District	33207
Mead School District	32354
Medical Lake School District	32326
Naches Valley School District	39003
Newport School District	26056
Northport School District	33211
Pomeroy School District	12110
Reardan-Edwall School District	22009
Republic School District	10309
Riverside School District	32416
Selah School District	39119
Selkirk School District	26070
Spokane School District	32081
St. John School District	38322
Sunnyside School District	39201
Tekoa School District	38265
Wapato School District	39207
Wellpinit School District	33049
West Valley School District (Spokane)	32363
West Valley School District (Yakima)	39208
Yakima School District	39007
Zillah School District	39205

College Partners (n=3)

College Name	College ID
Spokane Community College	171
Spokane Falls Community College	172
Yakima Valley Community College	160

DSA No. K1177

EXHIBIT D – Data Requested **Last Revised: 10/2/2014**

Three related files are requested: Students, CTCStudentIDs, and HSGradeHistory.

Student File

Locate all students who attended a high school within the K-12 districts listed in Exhibit C as seniors (CEDARS Element **B13 = 12**), between the School Years **2006** and the most recent full school year (2014 at this writing). Create **one record per student** based on the data associated with the **last high school attended**. Exclude exchange students and students who are attending part time (CEDARS: if B22>0 or B23>0 or B24<>N → exclude).

STUDENT FILE				
Data Element Name	**Element ID**	**Element Description**	**Format/Values**	**Comments**
SchoolYear	CEDARS B01	4-digit year in which the school year ends	Text (YYYY)	
CountyDistrictCode	CEDARS B02	5-character OSPI District ID (County/District)	Text	
DistrictStudentID	CEDARS B04	ID assigned to the student by the district	Text	
StateStudentID	CEDARS B05	ID assigned to the student by OSPI	Text	
DistrictName	CEDARS A03	District Name	Text	
LastHSCode	CEDARS A05	4-character OSPI school code of last HS attended	Text	
LastHSName	CEDARS A06	Name of last high school attended	Text	
LastName	CEDARS B06		Text	
FirstName	CEDARS B07		Text	
MiddleName	CEDARS B08		Text	
BirthDate	CEDARS B09		Date (MM/DD/YYYY)	
Sex	CEDARS B12		M or F	
HomelessStatus	CEDARS B21		Text	
HispanicEthnicity	CEDARS L05	Derived field: if L05<>10 then Y else N	Y or N	
RaceCode	CEDARS M05		text	
FreeReduced	CEDARS I06/I10	Derived Field: if I06=19 then I10 else blank	text	
CumHSGPA	CEDARS B28		Decimal	
CumHSCrdsAttempted	CEDARS B29		Decimal	
CumHSCrdsEarned	CEDARS B30		Decimal	
HSExitDate	CEDARS C08		Date (MM/DD/YYYY)	
HSWithdrawalCode	CEDARS C09		Text	

HSGradeHistory File

For each student in the STUDENT FILE, generate a set of records for all the high school credit classes taken by the student.

HSGradeHistory FILE				
Data Element Name	**Element ID**	**Element Description**	**Format/Values**	**Comments**
CountyDistrictCode	CEDARS H02	5-character OSPI District ID (County/District)	Text	
DistrictStudentID	CEDARS H03	ID assigned to the student by the district	Text	
CourseID	CEDARS H07		Text	
CourseTitle	CEDARS H08		Text	
GradeLevelCode	CEDARS H09		Text	
LetterGrade	CEDARS H10		Text	
CreditsAttempted	CEDARS H11		Decimal	
CreditsEarned	CEDARS H12		Decimal	
CourseDesignation	CEDARS H13		Text	
ContentAreaCode	CEDARS H14		Text	
StateCourseCode	CEDARS H15		Text	
APCourseCode	CEDARS H16		Decimal	
CIPCode	CEDARS H17		Text	
SchoolYear	CEDARS H01		Text (YYYY)	
Term	CEDARS H19		Text	
SchoolCode	CEDARS H26		Text	

CTCStudentID File

For each student in the STUDENT FILE, identify whether the student attended any of the community and technical colleges listed in Exhibit C. Create as many records as required to contain the Student IDs associated with each college.

CTCStudentID FILE				
Data Element Name	**Element ID**	**Element Description**	**Format/Values**	**Comments**
CountyDistrictCode	CEDARS B02	5-character OSPI District ID (County/District)	Text	
DistrictStudentID	CEDARS B04	ID assigned to the student by the district	Text	
CTCID		College code identifying the community/technical college	Text	
CTCName		Name of the community/technical college	Text	
CTCStudentID		ID assigned by the community/technical college attended	text	