DATA BRIEF

FEBRUARY 8, 2022

ACCESS TO CTCLINK INFRASTRUCTURE DATA MOU SUMMARY AND SOLUTIONS

Executive Summary

ctcLink administrative systems — Campus Solutions, Human Capital Management, and Finance — incorporate all community and technical college data into a single database. While a centralized system brings with it many benefits, it raises concerns about data privacy. College employees with designated security rights have the ability to see other colleges' data. For instance, during training and troubleshooting activities, it is more effective for ctcLink staff to work with Subject Matter Experts across the college system rather than by individual college. This means that during a training exercise or troubleshooting an issue, employees may see another college's data as they work through the activity.

A centralized system like ctcLink creates the need for the community and technical college system to implement policies and procedures concerning data privacy and usage, especially for student privacy under the Family Educational Rights and Privacy Act (FERPA). FERPA regulations restrict access to student data to any external entity unless a FERPA exemption allows for the activity.

To address data privacy and to ensure it's held in confidence, the Data Governance Committee worked with the community and technical college system's assistant attorney general, David Stolier, to draft a system-wide Memorandum of Understanding (MOU) to specify the FERPA exemption that would allow for specific activities defined as training and troubleshooting. By deeming college and State Board staff as "School Officials" while training or troubleshooting, we can apply this FERPA exemption.

In addition to the MOU policy, the Data Governance Committee developed a supporting procedure. The Data Usage and Privacy Agreement supports the MOU and is the mechanism to inform staff of the required and ethical use of data collected in ctcLink. The ctcLink Employee Data Privacy and Usage Agreement procedure requires employees to agree to keep data private and use it only in the course of their job duties.

The Data Governance Committee also proposed collecting employee attestations to a new Data Usage and Privacy Statement through the use of a pop-up form in the ctcLink Portal presented to staff upon their first log in after implementation and annually thereafter. The EMPLID and date of agreement will be stored in a custom table that will be replicated to dataLink for college access.

Approved Solution

The proposal for a pop-up form in ctcLink to collect employee attestations to the Data Usage and Privacy Agreement was presented to and approved by the ctcLink Working Group in September, 2021 (Log # 123).

The Washington Association of Community and Technical Colleges (WACTC) in January 2022

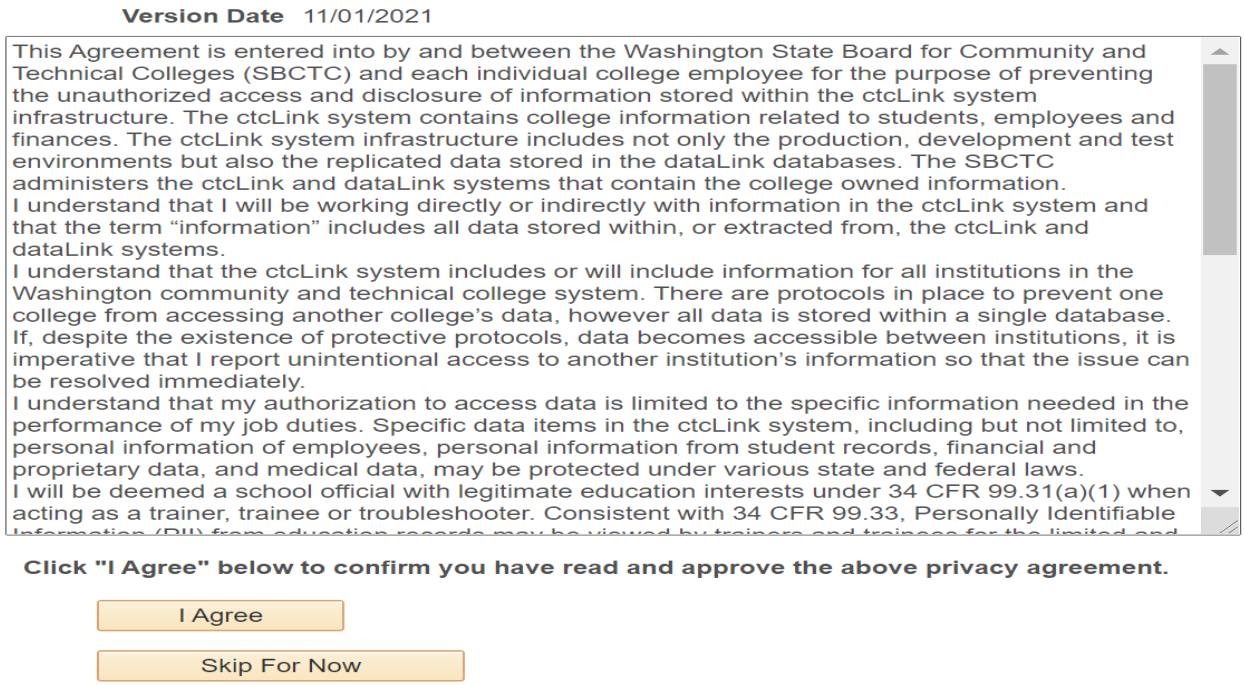
approved the Data Governance Committee's-proposed Memorandum of Understanding, Data Usage and Privacy Agreement, and pop-up form to collect employee attestations. The MOU and agreement apply to all college and State Board staff.

The Memorandum of Understanding is available in Appendix A and the Data Usage and Privacy Statement is available in Appendix B. Both documents are available on the SBCTC website here: https://www.sbctc.edu/colleges-staff/it-support/erp-support/data-privacy.aspx

What does this mean to me?

After implementation, each user who logs into ctcLink will be presented a pop-up form displaying the Data Usage and Privacy Agreement as shown below. This form is anticipated it to be implemented shortly after the last college has gone live on ctcLink in the spring of 2022.

Figure 1. ctcLink Data Usage and Privacy Agreement



- After the user attests to the agreement, they will continue the log in process to ctcLink as usual. Agreeing to this statement does not alter access or security in any way.
- If the user does not attest to the agreement, they may close the pop-up form and continue with the log in process as usual.
    - The pop-up form will continue to be presented to the user during each log-in until they have agreed to the statement.
- The user will be presented the pop-up form annually from the day of agreement thereafter.
- Queries will be available in ctcLink for security and HR staff to identify which employees have or have not agreed to the Data Usage and Privacy Statement.

Appendix A

Memorandum of Understanding Regarding Access to ctcLink Infrastructure Data

Last Updated June 12, 2021

THIS Memorandum Of Understanding is made and entered into by and between the following Washington state public institutions and agencies:

Bates Technical College
Bellevue College
Bellingham Technical College
Big Bend Community College
Cascadia College
Centralia College
Clark College
Clover Park Technical College
Columbia Basin College
Edmonds College
Everett Community College
Grays Harbor College
Green River College
Highline College
Lake Washington Institute of Technology
Lower Columbia College
North Seattle College
Seattle Colleges District Office
Olympic College
Peninsula College
Pierce College
Renton Technical College
Seattle Central College
Shoreline Community College
Skagit Valley College
South Puget Sound Community College
South Seattle College
Spokane Community College
Spokane Falls Community College
Community Colleges of Spokane
State Board for Community and Technical Colleges (SBCTC)
Tacoma Community College
Walla Walla Community College
Wenatchee Valley College
Whatcom Community College
Yakima Valley College

This Memorandum of Understanding (MOU) is entered into in accordance with, 20 U.S.C. § 1232g(b)(1)(F) and 34 C.F.R. § 99.31 of the Family Educational Rights and Privacy Act (FERPA) related to student information, the Federal Privacy Act, RCW 42.56.590 (9) related to disclosure of personal information requiring data breach notification, and other laws that make certain personal and financial transaction information confidential.

This MOU is effective this 26 day of January 2022.

IT IS THE SOLE PURPOSE OF THIS MOU to memorialize the obligations of the parties to this MOU regarding the safeguarding of information and data in the ctcLink system.

THEREFORE, IT IS MUTUALLY AGREED THAT:

All individuals with authorized access to information in the ctcLink system are required to sign an Employee Data Privacy and Usage Agreement attesting that the policies, guidelines and procedures found within have been have been made available for adequate review and consideration prior to access to the ctcLink system.

"Individuals" with authorized access include employees, staff, faculty, contractors, subcontractors, and any other person to whom a party to this agreement grants access to the ctcLink system and the data and information contained therein.

All obligations of confidentiality and non-disclosure apply to any and all data, not simply the data of the individual's institution. Thus, any data to which an authorized individual may be exposed, whether from their institution, or another institution, will always be treated consistently with regard to confidentiality, non-disclosure, and any related state or federal regulations. Further, any access or exposure of another institution's data to an unauthorized individual will be reported to the appropriate parties as indicated herein.

Obligation of Partners

1. Records, information, and data of the parties may be disclosed to the State Board for Community and Technical Colleges (SBCTC) for use in the ctcLink system. Student records may be disclosed to the SBCTC under the authority of 34 C.F.R § 99.31(a)(3) and § 99.31(a) (6)(i)(B). Data contained in ctcLink may contain confidential or personally identifiable information; no such information will be disclosed to any non-representative of the participating parties or in any analysis or publication. Personally or individually identifiable information will only be used for official and authorized purposes, including but not limited to the creation of a student identifier for the purpose of linking enrollment records across institutions. In accordance with 20 U.S.C. § 1232g(b)(1)(F) and 34 C.F.R. § 99.31(a)(6)(iii)(B) and 99.33(b), the SBCTC will, in consultation with the parties to this MOU as provided herein, destroy any individually identifiable information it receives under this agreement when it is no longer needed for the purposes of this MOU.

2. Due to the capabilities of the ctcLink system, each party to this MOU may be capable of accessing certain data through ctcLink that belongs to other institutions. With respect to personally identifiable student information (PII) from education records, under 34 CFR 99.31(a)(1), an educational institution that does not use physical or technological access controls must ensure that it has in place an effective administrative policy for controlling access. Accordingly, the data of other institutions shall not be accessed absent legal authority to do so. All access to such data will be conducted in accordance with the terms and obligations of this MOU and any associated Data Privacy and Usage Agreements.

3. The SBCTC procured ctcLink as a system-wide solution for the community and technical college (CTC) system. The phased rollout to the various colleges includes training and trouble-shooting that is carried out college to college by employees within the system rather than by contractors from outside the system. When acting in their capacity as trainers and troubleshooters, system employees may be deemed school officials of the trainee with legitimate education interests under 34 CFR 99.31(a)(1). Similarly, when being trained, trainee college employees may be deemed school officials of the trainer college for the limited purpose of viewing the live manipulation of demonstration data owned by the trainer college. Consistent with 34 CFR 99.33, PII from education records may be viewed by trainers and trainees for the limited and sole purposes of carrying out the training and troubleshooting activities. Such data must not be retained beyond the training activity and may not be further disclosed.
4. The parties agree to maintain the confidentiality of student educational records required by FERPA and maintain the confidentiality of other personally identifiable, sensitive, or protected information by maintaining policies that:
    a. Restrict linking the data found in ctcLink to any other data source unless needed to conduct official business,
    b. Restrict access to only designated individuals at the educational institutions involved who will use the data and information only in the course of performing their official duties,
    c. Require all individuals with access to information or data in ctcLink to sign an Employee Data Privacy and Usage Agreement,
    d. Adhere to all state and federal regulations regarding use of student data,
    e. Adhere to all state and federal regulations regarding use of employee data,
    f. Adhere to all state and federal regulations regarding use of financial data.
    g. Disclose data security breaches in accordance with RCW 42.56.590.
    h. Ensure employees are trained on their institutional data usage and privacy policies.
5. No institution shall publicly disclose another institution's data without prior written consent obtained from the appropriate authorities.

Reporting

Parties to this MOU shall comply with RCW 42.56.590 in the event of a data breach or unauthorized acquisition of data. Parties shall report to SBCTC in writing any unauthorized use, access, or disclosure of another institution's data not authorized by this MOU or associated Non Employee Data Usage Agreements. The parties discovering such incidents shall first make the disclosure to their college's designated ctcLink Security Administrator. If the report is deemed applicable, the college will make the disclosure to SBCTC in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement. This same report must also be shared with any college whose data was inappropriately

accessed.

The report shall identify where possible:

a. The nature of the unauthorized use or disclosure,

b. A description of the data or information used or disclosed,

c. Who made the unauthorized use or received the unauthorized disclosure,

d. Actions taken to mitigate any deleterious effect of the unauthorized use or disclosure,

e. What corrective action taken or anticipated to prevent future similar unauthorized use or disclosure.

Term

Subject to its other provisions and signing the MOU, the term of this MOU shall commence on January 26, 2022. This MOU will continue as long as the parties to this MOU have access to ctcLink data and information. The term does not affect the provisions of this MOU which are intended to survive the MOU, as identified in the section entitled "Survivorship."

Data and Information Handling Upon Termination

Upon expiration or termination of this MOU, Parties to this MOU shall certify that they have appropriately deleted and destroyed all confidential and personally identifiable data it no longer needs for authorized activities from its servers. Parties may request the return of their institutional data; any costs incurred for the retrieval, encryption, and delivery of that data will be the responsibility of the requesting Party.

Data on backup tapes stored in secure off-site locations will be deleted and scrubbed during the normal backup tape rotation schedule.

Authorization of Access

Each party to this MOU is responsible for establishing internal processes and procedures for granting authorization to individuals to access ctcLink data, for the training of those individuals, and for ensuring that those individuals have signed appropriate Employee Data Privacy and Usage Agreement. Parties to this MOU should conduct periodic review of lists of individuals with access, access granting procedures, training of individuals, and Employee Data Privacy and Usage Agreements and confidentiality policies.

Independent Capacity

The employees or agents of each party who are engaged in the performance of this MOU shall continue to be employees or agents of that party and shall not be considered for any purpose to be employees or agents of any other party to this MOU. The parties hereto, in the performance of this MOU, will be acting in their individual governmental capacities and not as agents, employees, partners, joint ventures, or associates of one another.

Liability

Each party shall be responsible for the actions and inactions of itself and its own officers, employees, and agents acting within the scope of their authority. The SBCTC reserves the right to suspend or terminate access to ctcLink from parties or individuals not in compliance with state and federal laws, regulations, or the terms of this MOU.

Survivorship

All ctcLink access shall be bound by all of the terms, conditions and obligations set forth herein, notwithstanding the expiration of the initial term of this MOU or any extension thereof. Further, the terms, conditions and obligations contained in this MOU that by their sense and context are intended to survive the completion of the performance, cancellation or termination of this MOU shall so survive. Obligations of the protection of personally identifiable information, confidential information, and other protected or sensitive data shall always survive the termination of this MOU. In addition, the terms of the sections titled OBLIGATION OF PARTNERS and REPORTING shall survive the termination of this MOU.

Appendix B

ctcLink Employee Data Privacy and Usage Agreement

Last Updated April 23, 2021

This Agreement is entered into by and between the Washington State Board for Community and Technical Colleges (SBCTC) and each individual college employee for the purpose of preventing the unauthorized access and disclosure of information stored within the ctcLink system infrastructure. The ctcLink system contains college information related to students, employees and finances. The ctcLink system infrastructure includes not only the production, development and test environments but also the replicated data stored in the dataLink databases. The SBCTC administers the ctcLink and dataLink systems that contain the college owned information.

I understand that I will be working directly or indirectly with information in the ctcLink system and that the term "information" includes all data stored within, or extracted from, the ctcLink and dataLink systems.

I understand that the ctcLink system includes or will include information for all institutions in the Washington community and technical college system. There are protocols in place to prevent one college from accessing another college's data, however all data is stored within a single database. If, despite the existence of protective protocols, data becomes accessible between institutions, it is imperative that I report unintentional access to another institution's information so that the issue can be resolved immediately.

I understand that my authorization to access data is limited to the specific information needed in the performance of my job duties. Specific data items in the ctcLink system, including but not limited to, personal information of employees, personal information from student records, financial and proprietary data, and medical data, may be protected under various state and federal laws.

I will be deemed a school official with legitimate education interests under 34 CFR 99.31(a)(1) when acting as a trainer, trainee or troubleshooter. Consistent with 34 CFR 99.33, Personally Identifiable Information (PII) from education records may be viewed by trainers and trainees for the limited and sole purposes of carrying out the training and troubleshooting activities. Such data must not be retained beyond the training or troubleshooting activity and may not be further disclosed.

I further understand that I am prohibited from directly or indirectly making any unauthorized disclosure of any such information to any other person or entity and I affirm and promise that I will not do so by complying with the following guidelines:

1. I will not purposefully access any information not required to fulfil my job duties.
2. I will not purposefully access, use or publish another institution's information.
3. I will access and retain data only for the period of time necessary to complete the job duties requiring me to access this data.
4. I will not save ctcLink data to personal devices unless required to complete my job duties and will

disposed of the information from those devices once it is no longer required.

5. I will not make any public disclosure or publication whereby individuals could be identified without the explicit authorization from my institution's administration.

6. I shall contact my college's ctcLink security administrator lead if I erroneously come into contact with another institutions information or information that I should not have access.

Any disclosure of information contrary to above is unauthorized and may trigger sanctions under state and federal law. Unauthorized disclosure of any confidential information will be referred to the employer for potential discipline and may be referred to the State Executive Ethics Board under RCW 42.52.050.

I am aware that I am accountable for all data usage policies, guidelines, and procedures that apply to my job duties at the organization. Moreover, I agree to use data in an appropriate and ethical manner including while training or troubleshooting. I understand that failure to abide by any and all policies, guidelines, and procedures can result in organizational, civil, or criminal action; and/or the termination of my employment.

I certify that I have been adequately trained by my employer in the application of these requirements and given ample opportunity to have any and all questions about my responsibilities addressed.

CONTACT INFORMATION
Carmen McKenzie
SBCTC Director of Data Services
dataservices@sbctc.edu