DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING
BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION ABOUT A CONTRACT
BETWEEN CAPITAL COMPUTER ASSOCIATES AND ONEIDA-HERKIMER-MADISON B

This Data Sharing and Confidentiality Agreement ("DSC Agreement") is made and entered into by and between Capital Computer Associates ("Vendor"), having its principal offices at 1 Antares Drive, Suite 400, Ottawa, ON, Canada, K2E8C4, and the Board of Cooperative Educational Services for the ONEIDA-HERKIMER-MAD ("BOCES"), having its principal offices at 4747 Middle Settlement Rd, New Hartford, NY 134 (collectively referred to as the "Parties").

1. Purpose and Term

(a) BOCES and Vendor are parties to an earlier agreement commencing on July 1, 2020 ("the Contract"). This DSC Agreement is entered into in order to conform the Contract to the requirements of New York State Education Law Section 2-d and Part 121 of the Regulations of the NYS Commissioner of Education (collectively referred to as "Section 2-d"). This DSC Agreement consists of the terms and conditions set forth herein, a copy of BOCES Bill of Rights for Data Security and Privacy signed by Vendor, and the "Supplemental Information about a Contract between Vendor and BOCES" that is required to be posted on BOCES' website.

(b) By affixing their signatures to this DSC Agreement below, BOCES and Vendor agree that the term of this DSC Agreement shall commence as of the date of mutual execution of this DSC Agreement by the Parties, and shall continue through and until the date of expiration of the Contract (or, through and until the date of expiration of an authorized renewal term or other authorized amendment of the Contract, if any) (the "Term"). Vendor shall comply with all terms, conditions and obligations as set forth in this DSC Agreement, including those set forth in BOCES' Bill of Rights for Data Security and Privacy and the Supplemental Information about a Contract between Vendor and BOCES, throughout the duration of the Term of this DSC Agreement, and this DSC Agreement shall supersede and take the place of any DSC Agreement entered into, or any similar data sharing and confidentiality language previously agreed to by the Parties (within the Contract or otherwise), prior to the date of mutual execution of this DSC Agreement.

(c) To the extent that any terms contained within the Contract, or any terms contained within any other agreements or exhibits attached to and made a part of the Contract, conflict with the terms of this DSC Agreement, the terms of this DSC Agreement will apply and be given effect. In the event that Vendor has online or written Privacy Policies or Terms of Service (collectively, "TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the Contract, to the extent that any term of the TOS (in effect as of the date of commencement of the Contract, and/or as subsequently amended) conflicts with the terms of this DSC Agreement, the terms of this DSC Agreement will apply and be given effect.

2. Definitions

Any capitalized term used within this DSC Agreement that is also found in the Contract, if any, will have the same definition as contained within the Contract.

In addition, as used in this DSC Agreement:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the Contract.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the Contract.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

(d) "Participating Educational Agency" means a school district within New York State that purchases certain shared technology services and software through a Cooperative Educational Services Agreement ("CoSer") with BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of the Contract. For purposes of this DSC Agreement, the term also includes BOCES if licensed to use Vendor's Product pursuant to the Contract to support its own educational programs or operations.

(e) "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1."

3. Confidentiality of Protected Data

(a) Vendor acknowledges that the Protected Data it receives pursuant to the Contract may originate from several Participating Educational Agencies located within New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(b) Vendor will maintain the confidentiality of all Protected Data it receives in accordance with applicable federal and state law (including but not limited to Section 2-d) and this DSC Agreement, as may be amended by the parties. Vendor acknowledges that BOCES is obligated under Section 2-d to adopt a policy on data security and privacy, but that adoption may not occur until a date subsequent to the effective date of this DSC Agreement. BOCES will provide Vendor with a copy of its policy as soon as practicable following adoption, and Vendor and BOCES agree to engage in good faith negotiations to modify this DSC Agreement to the extent necessary to ensure the parties' continued compliance with Section 2-d. Such modifications will become binding on the parties when made in writing and signed by both Parties.

4. Vendor's Data Security and Privacy Plan

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data it receives from Participating Educational Agencies in accordance with BOCES' Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

(a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this DSC Agreement, consistent with BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in

conformance with all applicable federal, state, and local laws and the terms of this DSC Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.

(b) As contained in the NIST Cybersecurity Framework, in order to protect the security, confidentiality and integrity of the Protected Data that it receives under the Contract, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the Contract:

Data Security:

- Data-at-rest & data-in-transit is encrypted
- Data leak protections are implemented

Information Protection Processes and Procedures:

- Data destruction is performed according to contract and agreements
- A plan for vulnerability management is developed and implemented

Protective Technology:

- Log/audit records are ascertained, implemented, documented and reviewed according to policy
- Network communications are protected

Identity Management, Authentication and Access Control:

- Credentials and identities are issued, verified, managed, audited and revoked, as applicable, for authorized devices, processes and users
- Remote access is managed

(c) Vendor will comply with all obligations set forth in BOCES' "Supplemental Information about a Contract between Vendor and BOCES." below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

(e) Vendor_____will _X_ will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the Contract. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the Contract, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in the "Supplemental Information about a Contract between Vendor and BOCES," below.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this DSC Agreement.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the Contract is terminated or expires, as more fully described in the "Supplemental Information about a Contract between Vendor and BOCES," below.

5. Additional Statutory and Regulatory Obligations

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the Contract and the terms of this DSC Agreement:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the Contract.

(c) Not use Protected Data for any purposes other than those explicitly authorized in this DSC Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the Contract, unless:

(i) the parent or eligible student has provided prior written consent; or
(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in the "Supplemental Information about a Contract between Vendor and BOCES," below.

(g) Provide notification to BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this DSC Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse BOCES or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. Notification of Breach and Unauthorized Release

(a) Vendor shall promptly notify BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to BOCES by contacting , Scott Morris BOCES Data Privacy Officer, at 315-793-8565

(c) Vendor will cooperate with BOCES and provide as much information as possible directly to Scott Morris or designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist BOCES or its Participating Districts if they have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by BOCES, Vendor will promptly inform Scott Morris or designee.

(e) Vendor will consult directly with Scott Morris or designee prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

IN WITNESS WHEREOF, the Parties have caused this DSC Agreement to be executed by their duly authorized representatives as of the dates set forth below.

CAPITAL COMPUTER ASSOCIATES, INC.

By: 

Printed Name: Gary Evans

Title: Executive Vice President

Date: April 16, 2021

DATA SHARING AND CONFIDENTIALITY AGREEMENT (CONTINUED)

BOCES

BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record.

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

(4) A complete list of all student data elements collected by the State is available for public review at http://www.nysed.gov/data-privacy-security/student-data-inventory, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website: http://www.nysed.gov/data-privacy-security/report-improper-disclosure.

BY THE VENDOR:

CAPITAL COMPUTER ASSOCIATES, INC.

By: 

Printed Name: Gary Evans

Title: Exective Vice President

Date: April 16, 2021

SUPPLEMENTAL INFORMATION ABOUT A CONTRACT
BETWEEN CAPITAL COMPUTER ASSOCIATES AND ONEIDA-HERKIMER-MAI BOCES

BOCES has entered into a Contract with Capital Computer Associates which governs the availability to Participating Educational Agencies of the following Product(s):

WinCap

Pursuant to this Contract, Participating Educational Agencies (*i.e.*, those educational agencies that are authorized to use the above Product(s) by purchasing certain shared technology services and software through a Cooperative Educational Services Agreement with BOCES) may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data"). Vendor has also entered into a separate Data Sharing and Confidentiality Agreement ("DSC Agreement") with BOCES setting forth Vendor's obligations to protect the confidentiality, privacy and security of Protected Data it receives pursuant to the Contract.

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to the Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized above or in the DSC Agreement. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized persons or entities i, it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging their obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the Contract and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: Capital Computer does not utilize subcontractors

Duration of Contract and Protected Data Upon Expiration:

- The Contract commences on July 1, 2020 and renews annually.
- Upon expiration of the Contract without renewal, or upon termination of the Contract prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.
- In the event the Contract is assigned to a successor Vendor (to the extent authorized by the Contract), the Vendor will cooperate with BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon

request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of any APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.