Exhibit C

Education Law Section 2-d Contract Addendum

The parties to this Contract Addendum are the Ulster County Board of Cooperative Educational Services ("BOCES") and Custom Computer Specialists, Inc. ("Vendor"). BOCES is an educational agency, as that term is used in Section 2- d of the New York State Education Law ("Section 2-d") and its implementing regulations, and Vendor is a third-party contractor, as that term is used in Section 2-d and its implementing regulations. BOCES and Vendor have entered into this Contract Addendum to conform to the requirements of Section 2-d and its implementing regulations. To theextent that any term of any other agreement or document conflicts with the terms of this Contract Addendum, the terms of this Contract Addendum shall apply and be given effect.

Definitions

As used in this Addendum and related documents, the following terms shall have the following meanings:

"Student Data" means personally identifiable information from student records that Vendor receives from an educational agency (including BOCES or a Participating School District) in connection with providing Services under this Agreement.

"Personally Identifiable Information" ("PII") as applied to Student Data, means personally identifiable information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA), at 20 USC 1232g.

"Third Party Contractor," "Contractor" or "Vendor" means any person or entity, other than an educational agency, that receives Student Data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including, but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs.

"BOCES" means the Ulster County Board of Cooperative Educational Services.

"Parent" means a parent, legal guardian, or person in parental relation to a student.

"Student" means any person attending or seeking to enroll in an educational agency.

"Eligible Student" means a student eighteen years or older.

"State-protected Data" means Student Data, as applicable to Vendor's product/service.

"Participating School District" means a public school district or board of cooperative educational services that obtains access to Vendor's product/service through a cooperative educational services agreement ("CoSer") with BOCES, or other entity that obtains access to Vendor's product/service through an agreement with BOCES, and also includes BOCES when it uses the Vendor's product/service to support its own educational programs or operations.

"Breach" means the unauthorized access, use, or disclosure of Student Data by or to a person not authorized to acquire, access, use, or receive the Student Data.

"Commercial or marketing purpose" means the sale of Student Data; and the direct or indirect use or disclosure of State- protected Data to derive a profit, advertise, or develop, improve, or market products or services to students other than as may be expressly authorized by the Student Management Services Agreement (the "Services").

"Disclose", "Disclosure," and "Release" mean to intentionally or unintentionally permit access to State-protected Data; and to intentionally or unintentionally release, transfer, or otherwise communicate State-protected Data to someone not authorized by contract, consent, or law to receive that State-protected Data.

Vendor Obligations and Agreements

Vendor agrees that it shall comply with the following obligations with respect to any Student Data received in connection with providing Services under this Agreement and any failure to fulfill one of these statutory orregulatory obligations shall be a breach of this Agreement. Vendor shall:

(a) limit internal access to education records only to those employees and subcontractors that are determined to have legitimate educational interests in accessing the data within the meaning of Section 2-d, its implementing regulations and FERPA (e.g., the individual needs access in order to fulfill his/her responsibilities in providing the contracted services);

(b) only use personally identifiable information for the explicit purpose authorized by the Agreement, and must/will not use it for any purpose other than that explicitly authorized in the Agreement;

(c) not disclose any personally identifiable information received from BOCES or a Participating School District to any other party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Agreement, unless (i) if student PII, the Vendor or that other party has obtained the prior written consent of the parent or eligible student, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

(d) maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the personally identifiable information in its custody;

(e) Infinite Campus Cloud Hosting uses encryption technology to protect data while in motion or in its custody (i.e., in rest) from unauthorized disclosure by rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5 using a technology or methodology specified or permitted by the secretary of the U S.);

(f) not sell personally identifiable information received from BOCES or a Participating School District nor use or disclose it for any marketing or commercial purpose unless otherwise expressly authorized by the Services, or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;

(g) notify the educational agency from which Student Data is received of any breach of security resulting in an unauthorized release of such data by Vendor or its assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay, in compliance with New York law and regulation;

(h) reasonably cooperate with educational agencies and law enforcement to protect the integrity of investigations into any breach or unauthorized release of personally identifiable information by Vendor;

(i) adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework, Version 1.1, that are in substantial compliance with the BOCES data security and privacy policy, and that comply with Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education and the BOCES Parents' Bill of Rights for Data Privacy and Security, set forth below, as well as all applicable federal, state andlocal laws, rules and regulations;

(j) acknowledge and hereby agrees that the State-protected Data which Vendor receives or has access to pursuant to this Agreement may originate from several Participating School Districts located across New York State. Vendor acknowledges that the State-protected Data belongs to and is owned by the Participating School District or student from which it originates;

(k) acknowledge and hereby agrees that if Vendor has an online terms of service and/or Privacy Policy that may be applicable to its customers or users of its product/service, to the extent that any term of such online terms of service or Privacy Policy conflicts with applicable law or regulation, the terms of the applicable law or regulation shall apply;

(l) acknowledge and hereby agrees that Vendor shall promptly pay for or reimburse the educational agency for the full third party cost of a legally required breach notification to parents and eligible students due to the unauthorized release of Student Data caused by Vendor or its agent or assignee;

(m) ensure that employees, assignees and agents of Vendor who have access to Student Data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access to such data; and

(n) ensure that any subcontractor that performs Vendor's obligations pursuant to the Agreement is legally bound by legally compliant data protection obligations imposed on the Contractor by law, the Agreement and this Addendum.

(o) Vendor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record, or display any State-protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Vendor will receive under the contract;
2. Demonstrates Vendor's compliance with the requirements of Section 121.3 of Part 121;
3. Specifies how officers or employees of the Vendor and its assignees who have access to Student Data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
4. Specifies how Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
5. Specifies how Vendor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;
6. Specifies whether State-protected Data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the contract is terminated or expires.

Supplemental Information About Agreement Between Custom Computer Specialists, Inc. and BOCES

(a) The exclusive purposes for which the personally identifiable information provided by BOCES or a Participating School District will be used by Vendor is to provide the products and services described in Exhibit A to the Student Management System Services Agreement with BOCES or other Participating School District pursuant to a BOCES Purchase Order.

(b) Personally identifiable information received by Vendor, or by any assignee of Vendor, from BOCES or from a Participating School District shall not be sold or used for marketing purposes.

(c) Personally identifiable information received by Vendor, or by any assignee of Vendor shall not be shared with a sub-contractor except pursuant to a written contract that binds such a party to at least the same data protection and security requirements imposed on Vendor under this Agreement, as well as all applicable state and federal laws and regulations.

(d) The effective date of this Contract Addendum shall be July 1, 2021. The term of the Agreement is from July 1, 2021 through June 30, 2022 unless terminated earlier in accordance with its terms.

(e) Upon expiration or termination of the Agreement without a successor or renewal agreement in place, and upon request from BOCES or a Participating School District, Vendor shall transfer all educational agency data to the educational agency in a format agreed upon by the parties. Vendor shall thereafter securely delete all educational agency data remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies) as well as any and all educational agency data maintained on behalf of Vendor in secure data center facilities, other than any data that Vendor is required to maintain pursuant to law, regulation or audit requirements. Vendor shall ensure that no copy, summary or extract of the educational agency data or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the secure data center facilities unless Vendor is required to keep such data for legal, regulator, or audit purposes, in which case the data will be retained in compliance with the terms of this Addendum. To the extent that Vendor and/or its subcontractors or assignees maycontinue to be in possession of any de-identified data (data that has had all direct and indirect identifiers permanently removed with no possibility of reidentification), they each agree not to attempt to re-identify de- identified data and not to transfer de-identified data to any party. Upon request, Vendor and/or its subcontractors orassignees will provide a certification to the BOCES or Participating School District from an appropriate officer that the requirements of this paragraph have been satisfied in full.

(f) State and federal laws require educational agencies to establish processes for a parent or eligible student to challenge the accuracy of their Student Data. Third party contractors must cooperate with educational agencies in complying with the law. If a parent or eligible student submits a challenge to the accuracy of Student Data to the student's district of enrollment and the challenge is upheld, Vendor will cooperate with the educational agency with respect to such challenge, which shall be handled in accordance with the educational agency's applicable policies and procedures.

(g) Vendor shall store and maintain PII in electronic format on systems maintained by Vendor in a secure data center facility in the United States in accordance with its Privacy Policy, aligns with NIST Cybersecurity Framework, Version 1.1, and the BOCES data security and privacy policy, Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education, and the BOCES Parents' Bill of Rights for Data Privacy and Security, set forth above. Encryption technology will be utilized while data is in motion and at rest, as detailed above.

J. P. Nel

Digitally signed by f4aa7cb4-4a56-4026-a687-ecb29282f2e6
DN: cn=f4aa7cb4-4a56-4026-a687-ecb29282f2e6
Date: 2021.07.03 08:43:25 -04'00'

Vendor Signature

7/3/2021

Date

CUSTOM COMPUTER SPECIALISTS' AND ULSTER COUNTY BOCES' PLAN FOR SECURITY AND PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION

I. INTRODUCTION

For over 35 years, Custom Computer Specialists ("CCS") has provided information technology solutions to a wide variety of customers. CCS provides high quality education technology consulting and professional development to U.S. educational institutions. CCS is dedicated to helping educational agencies maximize their use of technology in the classroom and campus-wide. As an expert in educational consulting, CCS provides education technology consulting and implementation in schools.

CCS has entered into an Agreement with **ULSTER COUNTY BOCES** ("BOCES") dated **July 1, 2021** to provide record and data management services for certain of BOCES' component districts ("End Users") (the terms, BOCES and End Users, collectively will be referred to as "Educational Agencies" or "EAs"). CCS will provide or has provided services to End Users to implement End User-wide student information systems ("SISs") provided by Infinite Campus (the Infinite Campus SIS is sold by and provided to the End Users pursuant to agreements between Infinite Campus and BOCES or the End Users). After implementation of an SIS, CCS will provide the End User with development, consulting and user support services. Due to the nature of the services CCS will provide for the End Users, CCS and/or its employees will receive and/or have access to personally identifiable information from the End User's students records ("PII").

II. PERSONALLY IDENTIFIABLE INFORMATION

Personally identifiable information includes, but is not limited to: a student's name; the name of a student's parent or other family members; a student's address; any personally identifiable information (e.g., student's SSN, student number or biometric record); indirect identifiers *(e.g.,* student's date of birth, place of birth, or mother's maiden name); other information that alone or in combination is linked or linkable to a specific student and would allow a reasonable person to identify the student with reasonable certainty; and any information requested by a person who BOCES or an End User reasonably believes knows the identity of the student to whom a record relates.

III. PLAN FOR SECURITY AND PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION

A. **Compliance with EA Policies and the Law** - CCS will comply with all BOCES policies and regulations provided by BOCES to CCS prior to the execution of the Agreement and, upon notification and CCS' written agreement to same, all amendments to those policies or regulations or other applicable and reasonable BOCES policies or regulations provided by BOCES to CCS thereafter. Upon notification and CCS' written agreement to same, CCS will also comply with all applicable and reasonable End User policies and regulations provided by BOCES or an End User to CCS. CCS and BOCES will comply with all applicable State and federal laws, regulations, rules, and requirements related to the confidentiality of records and data security and privacy.

Pursuant to New York State Education Law § 2-d ("§ 2-d"), CCS will:

1. Limit internal access to data or records of the EAs that are deemed confidential pursuant to State or federal law ("EA Records") and PII to individuals with legitimate educational interests *(i.e.*, access will be limited to those individuals who must access EA Records and PII to implement the terms of the Agreement);

2. Use EA Records and PII only for the purposes explicitly authorized by the Agreement;

3. Not disclose PII to any other party who is not an authorized representative of CCS without prior written consent of the parent or eligible student (if necessary, CCS will request this consent from the EAs), unless disclosure is required by statute or court order and written notice is given to the End User's Board of Education (notice will not be given to the End User's Board of Education by CCS if it is expressly prohibited by a statute or court order);

   ***Note 1:** Custom does develop integrations to enable data sharing with other third party vendors on request of districts or BOCES. Custom will only develop such integrations with a written request from the districts or BOCES. It will be the district's and/or BOCES responsibility to ensure that these vendors have data protection and security agreements in place.*
   ***Note 2:** Custom does not make use of sub-contractors to perform services, but if required, will collaborate with the district and EAs to ensure compliance to all legal requirements.*

4. Maintain reasonable administrative, technical and physical safeguards to maintain confidentiality of PII;

5. Use legally mandated encryption technology to protect PII from unauthorized disclosure; and

6. Not sell PII or use PII for marketing purposes.

B. **Parents' Bill of Rights** – BOCES' Parents' Bill of Rights is annexed hereto as Exhibit A As required by § 2-d(3)(c), the BOCES' Parents' Bill of Rights is supplemented with the following information:

1. The exclusive purposes for which PII will be used pursuant to the Agreement;

2. How CCS will ensure the confidentiality of PII that is shared with subcontractors or other persons or entities by CCS;

3. What happens to PII upon expiration of the Agreement;

4. If and how a parent, student, teacher or principal may challenge the accuracy of the collected PII; and

5. Where the PII will be stored and what security protections will be taken by CCS.

C. **Training** -Pursuant to § 2-d(5)(e), CCS will provide training about the applicable State and federal laws and regulations relating to confidentiality of PII to any employee who has access to PII.

All employees supporting Infinite Campus completes online training.
All Officers and Employees are briefed during quarterly department meetings on handling PII. All staff are informed (at a minimum once per year) via email on the latest Data Privacy and Security requirements and measures used by CCS.

Custom does not make use of sub-contractors to perform services, but if required, CCS will collaborate with the district and EAs to ensure compliance to all legal requirements; including training.

D. **Notification of Breach** – Pursuant to § 2-d(6), CCS will notify BOCES of any breach of security resulting in an unauthorized release of PII by CCS. This notification will be made in the most expedient way possible and without delay.

E. **Destruction of PII** - Upon termination of the Agreement for any reason during a period of time that PII and EA Records are hosted and/or stored by CCS, CCS will destroy all PII and EA Records as soon as reasonably possible and agreed upon between CCA and EA. If requested by BOCES in writing, CCS will provide a certificate of destruction.

EXHIBIT A

TO

PLAN FOR SECURITY AND PROTECTION

OF PERSONALLY IDENTIFIABLE INFORMATION

This Bill of Rights is supplemented to include the following information about the Agreement between Custom Computer Specialists ("CCS") and the ULSTER COUNTY BOCES ("BOCES");

(1) PII Used by CCS: PII received by CCS pursuant to the Agreement between CCS and BOCES ("the Agreement") will be used for the following purposes:

(a) Data Conversion/SIS Implementation Phase: CCS will provide services to implement Infinite Campus student information systems ("SISs") for certain of BOCES' component districts ("End Users") (the terms, BOCES and End Users, collectively will be referred as "Educational Agencies" or "EAs"). CCS will perform an initial data conversion to conform an End User's existing data for use by the Infinite Campus SIS. CCS will receive the End User's data from the End User and store it in a secure development environment hosted by CCS.

(b) Development and Testing Phase: After the data is converted the End User will run tests and ensure that the Infinite Campus SIS is ready to be used by the EA.

(c) Support Services Phase: After the Infinite Campus SIS has gone live an is in use, CCS will provide consulting, development and user support services to the End User in connection with the End User's use of the Infinite Campus SIS. These services include, but are not limited to, general user support creation of customized reports and Conformance of data to enable the End User's data to interface with programs of other vendors (e.g., a food service contractor) (any data conversion and/or sharing of data with a third-party vendor (other than Infinite Campus will be not be performed by CCS)). During this stage, all PII and data or records of the EAs that are deemed confidential pursuant to State or federal law ("EA Records") will be stored and/or hosted by Infinite Campus on Infinite Campus-owned equipment or in the Cloud. CCS will have access to the PII and EA Records and may temporarily possess the data to assist an End User with resolving a problem and to carry out CCS' other support service-related obligations.

(2) PII Storage/Security Protections: End User data will be sent to CCS by the End User through a secure file transfer over a SFTP site. During the Data Conversion/Implementation Phase and the subsequent holding period (*see* 3(a) below), the data received by CCS will be stored by CCS in a secure development environment hosted by CCS. CCS will limit physical access to this environment through premises security and the use of firewalls and passwords. Only employees who must access EA Records and PII to implement the terms of the Agreement will have access to the secure development environment. The converted data will be sent by CCS to Infinite Campus through a secure file transfer over a SFTP site. The data will be further protected through the use of encryption technology in compliance with New York Education Law§ 2-d(5)(f)(5).

(3) **Destruction of PII:**

(a) After the Data Conversion/SIS Implementation phase, the PII hosted by CCS will continue to be stored and hosted by CCS for a reasonable period of time during the initial period of the End User's use of the Infinite Campus SIS (typically, 60-90 days) ("the holding period"). This retention is done in case of any failures or problems discovered that require further data conversion and/or implementation services. After the holding period, CCS will shut down and disable the secure development environment and destroy all PU and EA Records. If requested by BOCES in writing, CCS will provide a certificate of destruction.

(b) Any PII or EA Records temporarily possessed by CCS during the Support Services Phase will be destroyed as soon as reasonably possible after the PII or EA Records are no longer needed. If requested by BOCES in writing, CCS will provide a certificate of destruction.

(c) Upon termination of the Agreement for any reason during a period of time that PII and EA Records are hosted and/or stored by CCS, CCS will destroy all PII and EA Records as soon as reasonably possible. If requested by BOCES in writing, CCS will provide a certificate of destruction.

(4) **Sharing Information with Other Entities and Non-CCS Employees:** CCS will only share PII or EA Records with Infinite Campus pursuant to the Agreement. To the extent that PII will be shared by CCS with other authorized entities or persons not employed by CCS, the PII will be shared pursuant to the terms of the Agreement. Those persons and/or entities will be required to agree in writing that it/they will comply with CCS' and BOCES' Plan for Security and Protection of Personally Identifiable Information. *Note: Custom does develop integrations to enable data sharing with other third-party vendors on request of districts or BOCES. Custom will only develop such integrations with a written request from the districts or BOCES. It will be the district's and/or BOCES responsibility to ensure that these vendors have data protection and security agreements in place.*

(5) **Challenge to Accuracy of PII Received by CCS:** A parent, student, teacher or principal can challenge the accuracy of the PII received by CCS pursuant to the Agreement by following applicable law *(e.g.,* FERPA), employment agreements, and policies, rules and regulations. If CCS receives a challenge to the accuracy of PII from a parent, student, teacher or principal, CCS will notify the EAs in writing. CCS will not amend any data received from an End User unless it receives a written request from that End User to make the requested change.

IRAN DIVESTMENT ACT OF 2012 CERTIFICATION

As a result of the Iran Divestment Act of 2012 (Act), Chapter 1 of the 2012 Laws of New York, added new provisions to the State Finance Law (SFL), §165-a and General Municipal Law (GML) §103-g effective April 12, 2012. Under the Act, the Commissioner of the Office of General Services (OGS) will be developing a list (prohibited entities list) of "persons" who are engaged in "investment activities in Iran" (both are defined terms in the law). Pursuant to SFL § 165-a(3)(b) and GML §103-g, the initial list is expected to be issued no later than 120 days after the Act's effective date, at which time it will be posted on the OGS website.

By submitting a response to this solicitation or by assuming the responsibility of a Contract awarded hereunder, Vendor (or any assignee) certifies that once the prohibited entities list is posted on the OGS website, it will not utilize on such Contract any subcontractor that is identified on the prohibited entities list.

Additionally, Vendor is advised that once the list is posted on the OGS website, any Vendor seeking to enter into, renew or extend a Contract or assume the responsibility of a Contract awarded in response to the solicitation, must certify at the time the Contract is bid upon or a proposal submitted, or the contract is renewed, extended or assigned that it is not included on the prohibited entities list.

During the term of the Contract, should BOCES receive information that a person is in violation of the above-referenced certification, BOCES will offer the person an opportunity to respond. If the person fails to demonstrate that it has ceased its engagement in the investment which is in violation of the Act within 90 days after the determination of such violation, then BOCES shall take such action as may be appropriate including, but not limited to, imposing sanctions, seeking compliance, recovering damages, or declaring the Vendor in default.

BOCES reserves the right to reject any bid, proposal or request for assignment for an entity that appears on the prohibited entities list prior to the award of a contract, and to pursue a responsibility review with respect to any entity that is awarded a contract and appears on the prohibited entities list after contract award.

Signature: _____

Print Name: Brad Page

Title: CFO

Company Name: Infinite Company, Inc

Date: 6/8/2021