EXHIBIT C
DATA PROTECTION ADDENDUM
Adlai E Stevenson High School District 125 – October 12, 2021

This Exhibit C ("Exhibit C") to the CIC Licensed Product Agreement ("Contract"), is by and between Computer Information Concepts, Inc., 2843 31st Avenue, Greeley, Colorado 80631 ("Contractor") and Adlai E Stevenson High School District 125, 1 Stevenson Drive, Lincolnshire, IL 60069-2824 ("District") and amends the agreement between the same parties titled Licensed Product Agreement dated December 19, 2008. This Addendum supersedes the Agreement by adding to, deleting from and modifying the Agreement as set forth herein. To the extent any such addition, deletion or modification results in any conflict or inconsistency between the Agreement and this Addendum, this Addendum shall govern and the terms of the Agreement that conflict with this Addendum or are inconsistent with this Addendum shall be of no force or effect. In consideration of the mutual covenants, promises, understandings, releases and payments described in the Agreement and this Addendum, the parties agree to amend the Agreement by adding the following language:

1. Definitions

1.1 "*Designated Representative*" means District or Contractor employees as specified on Schedule 1 to whom all notices required in this Addendum will be sent.

1.2 "*District Data*" means any Personally Identifiable Information, Record, Education Record and all Personally Identifiable Information included therein or derived therefrom that is not intentionally made generally available by the District on public websites or publications but is made available directly or indirectly by the District to Contractor or that is otherwise collected or generated by Contractor in connection with the performance of the Services. District Data includes any and all "covered information" as that term is defined in Section 5 of SOPPA (105 ILCS 85/5), and District Data shall constitute "school student records" as that term is defined in Section 2 of ISSRA (105 ILCS 10/2(d))

1.3 "*De-identified Data*" means District Data from which all personally identifiable information, as defined herein, and attributes about such data, have been permanently removed so that no individual identification can be made.

1.4 "*Education Records*" means records, files, documents and other materials that: (a) contain information directly related to a student; and (b) are maintained by the District, or by a party acting for the District such as Contractor.

1.5 "*End User*" means individuals authorized by the District to access and use the Services provided by the Contractor under the Contract.

1.6 "*Incident*" means a suspected, attempted, or imminent threat of unauthorized access, use, disclosure, breach, modification, disruption or destruction to or of District Data.

1.7 "*Mine District Data*" means the act of searching through, analyzing, accessing, or extracting District Data, metadata, or information not necessary to accomplish the Services or purpose(s) of this Agreement for the benefit of the District.

1.8 "*Personally Identifiable Information*" or "*PII*" means information and metadata that, alone or in combination, is linked or linkable to a specific student so as to 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. Personally identifiable information includes but is not limited to: (a) the student's name; (b) the name of the student's parent or other family members; (c) the address or phone number of the student or student's family; (d) personal identifiers such as the student's state-assigned student identifier, social security number, student number or biometric record; (e) indirect identifiers such as the student's date of birth, place of birth or mother's maiden name; and (f) demographic attributes, such as race, socioeconomic information, and gender.

1.9 "*Record*" means any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche.

1.10 "*Securely Destroy*" means to remove District Data from Contractor's systems, paper files, records, databases,

and any other media regardless of format, in accordance with the standard detailed in National Institute of Standards and Technology ("NIST") SP 800-88 Guidelines for Media Sanitization so that District Data is permanently irretrievable in Contractor's and its Subcontractors' normal course of business.

1.11 "*Security Breach*" means an event in which District Data is exposed to unauthorized disclosure, access, alteration or use or a system configuration that results in a documented unsecured disclosure, access, alteration or use, in a manner not permitted in this Addendum, which poses a significant risk of financial, reputational or other harm to the affected End User or the District.

1.12 "*Services*" means any goods or services acquired by the District from the Contractor, including computer software, mobile applications (apps), and web-based tools accessed by End Users through the Internet or installed or run on a computer or electronic device.

1.13 "*Subcontractor*" means Contractor's employees, subcontractors or agents, identified on Schedule 2, as updated by Contractor from time to time in accordance with the requirements of this Addendum, who Contractor has engaged to enable Contractor to perform its obligations under the Contract.

1.14 "*Student Profile*" means a collection of PII data elements relating to a student of the District.

2. Rights and License in and to District Data

District owns all rights, title, and interest in and to District Data. The District hereby grants to Contractor a limited, nonexclusive license to use District Data and De-identified Data solely for the purpose of performing its obligations specified in the Contract or as otherwise permitted by the Agreement. Contractor shall have no rights, title, or interest implied or otherwise, to District Data or De-identified Data, except as expressly stated in the Agreement.

3. Data Privacy

3.1 Use of District Data. Contractor shall use District Data only for the purpose of performing the Services and fulfilling its duties under the Contract.

3.2 Prohibited Uses of District Data. With the exception of De-identified Data that the District has agreed in writing to allow Contractor to use as specified in Section 3.5, Contractor shall not:

3.2.1 Use, sell, rent, transfer, distribute, alter, Mine, or disclose District Data (including metadata) to any third party without the prior written consent of the District, except as required by law;

3.2.2 Use District Data for its own commercial benefit, including but not limited to, advertising or marketing of any kind directed toward children, parents, guardians, or District employees, unless such use is specifically authorized by this Agreement or otherwise authorized in writing by the District;

3.2.3 Use District Data in a manner that is inconsistent with Contractor's privacy policy;

3.2.4 Use District Data to create a Student Profile other than as authorized or required by the District to perform the Services; and

3.2.5 Store District Data outside the continental United States unless Contractor has given the District Designated Representative advance written notice of where and how the servers are housed, managed, and secured, and that the security standards required herein can be achieved.

3.3 Qualified FERPA Exception. If Contractor will have access to Education Records, Contractor acknowledges that, for the purposes of this Agreement, pursuant to the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g and its implementing regulations, 34 C.F.R. Part 99 ("FERPA"), it will be designated as a "school official" with "legitimate educational interests" in the District Education Records and PII disclosed pursuant to the Contract, and Contractor agrees to abide by the FERPA limitations and requirements imposed on school officials. Contractor will use the Education Records only for the purpose of fulfilling its duties under the Contract. Contractor is performing an institutional service for which the school would otherwise use employees, is under the direct control of the District, for District's and its End Users' benefit, and shall not share District Data with or disclose it to any third party except as provided for in the Agreement, as

required by law, or if authorized in writing by the District. Contractor warrants and represents that during the five-year period preceding the Effective Date of this Agreement, it has not been found in violation of FERPA by the Family Policy Compliance Office.

3.4 Subcontractor Use of District Data. To the extent necessary to perform its obligations specified in the Contract, Contractor may disclose District Data to Subcontractors pursuant to a written agreement, specifying the purpose of the disclosure and providing that: (a) Subcontractor shall not disclose District Data, in whole or in part, to any other party; (b) Subcontractor shall not use any District Data to advertise or market to students or their parents/guardians; (c) Subcontractor shall access, view, collect, generate and use District Data only to the extent necessary to assist Contractor in performing its obligations specified in the Contract; (d) at the conclusion of its/their work under its/their subcontract(s) Subcontractor shall, as directed by the District through Contractor, Securely Destroy all District Data in its/their possession, custody or control, or return such District Data to the District, at the election of the District; (e) Subcontractor shall indemnify the District in accordance with the terms set forth in Section 10 herein below; and (f) Subcontractor shall utilize appropriate administrative, physical and technical safeguards in accordance with industry standards and best practices to secure District Data from unauthorized disclosure, access and use. Contractor shall ensure that its employees and Subcontractors who have access to District Data have undergone appropriate background screening, including Criminal Records Search, (County), SSN Death Master Search, Sex Offender Registry Search, and Smart Scan, and possess all needed qualifications to comply with the terms of this Addendum.

3.5 Use of De-identified Data. Contractor may use De-identified Data for purposes of research, the improvement of Contractor's products and services, and/or the development of new products and services. In no event shall Contractor or Subcontractors re-identify or attempt to re-identify any De-identified Data or use De-identified Data in combination with other data elements or De-identified Data in the possession of a third-party affiliate, thereby posing risks of re-identification.

3.6 Privacy Policy Changes. Prior to making a material change to Contractor's privacy policies, Contractor shall send District's Designated Representative written notice, which includes a clear explanation of the proposed changes.

4. Data Security

4.1 Security Safeguards. Contractor shall store and process District Data in accordance with commercial best practices, including implementing appropriate administrative, physical, and technical safeguards that are no less rigorous than those outlined in SANS Top 20 Security Controls, as amended, to secure such data from unauthorized access, disclosure, alteration, and use. Contractor shall ensure that all such safeguards, including the manner in which District Data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with all applicable federal and state data protection and privacy laws, regulations and directives, as well as the terms and conditions of this Addendum. Without limiting the foregoing, and unless expressly agreed to the contrary in writing, Contractor warrants that all electronic District Data will be encrypted in transmission and at rest in accordance with NIST Special Publication 800-53, as amended.

4.2 Risk Assessments. Contractor shall conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.

4.3 Audit Trails. Contractor shall take reasonable measures, including the availability of Data Change Tracker functionality (if purchased), to protect District Data against deterioration or degradation of data quality and authenticity.

4.4 Verification of Safeguards. Upon District's written request, Contractor shall provide or make available to the District for review, the following, verifying Contractor's administrative, physical and technical safeguards are in compliance with industry standards and best practices: (1) a third-party network security audit report, or (2) certification from Contractor indicating that an independent vulnerability or risk assessment of the Contractor's data security program has occurred.

5. Security Incident and Security Breach

5.1 Security Incident Evaluation. In the event of an Incident, Contractor shall follow industry best practices to fully investigate and resolve the Incident, and take steps to prevent developments that may result in the Incident becoming a Security Breach at Contractor's expense in accordance with applicable privacy laws.

5.2 Response. Immediately upon becoming aware of a Security Breach, or a complaint of a Security Breach, Contractor shall notify the District Designated Representative in writing as set forth herein, fully investigate the Security Breach, cooperate fully with the District's investigation of and response to the Security Breach, and use best efforts to prevent any further Security Breach at Contractor's expense in accordance with applicable privacy laws. Except as otherwise required by law, Contractor shall not provide notice of the Security Breach directly to individuals whose Personally Identifiable Information was involved, to regulatory agencies, or to other entities, without first providing written notice to the District's Designated Representative.

5.3 Security Breach Report. If the District reasonably determines that Contractor has committed a Security Breach, then the District may request Contractor to submit, within seven (7) calendar days from discovery of such breach, a written report, and any supporting documentation, identifying (i) the nature of the Security Breach, (ii) the steps Contractor has executed to investigate the Security Breach, (iii) what District Data or PII was used or disclosed, (iv) who or what was the cause of the Security Breach, (v) what Contractor has done or shall do to remediate any deleterious effect of the Security Breach, and (vi) what corrective action Contractor has taken or shall take to prevent a future Incident or Security Breach. The District reserves the right to require Contractor to amend its remediation plans.

5.4 Effect of Security Breach. Upon the occurrence of a Security Breach caused by inadequacies in Contractor's security systems, procedures, and or firewalls, the District may terminate this Agreement in accordance with District policies. The District may require Contractor to suspend all Services, pending the investigation and successful resolution of any Security Breach, and Contractor may be required to reimburse District all amounts paid for any period during which Services were not rendered, as provided herein. Contractor acknowledges that, as a result of a Security Breach, the District may also elect to disqualify Contractor and any of its Subcontractors from future contracts with the District. These provisions do not go into effect as a result of a Security Breach caused by the District or an individual user who self-compromises their own PII or user credentials.

5.5 Liability for Security Breach. In addition to any other remedies available to the District under law or equity, Contractor shall reimburse the District in full for all costs incurred by the District in investigation and remediation of any Security Breach caused by Contractor or Contractor's Subcontractors, including but not limited to providing notification to individuals whose Personally Identifiable Information was compromised and to regulatory agencies or other entities as required by law or contract.

6. Response to Legal Orders, Demands or Requests for Data

Note: In this section, when referring to data, it refers to data that is not customarily available to the district through the Student Information System. In most cases, the District will be able to access the data it needs as part of normal operations of the Student Information System.

6.1 Received by Contractor. Except as otherwise expressly prohibited by law, Contractor shall immediately notify the District of any subpoenas, warrants, other legal orders, or demands or requests received by Contractor seeking District Data; consult with the District regarding its response; cooperate with the District's reasonable requests in connection with efforts by the District to intervene and quash or modify the legal order, demand or request; and, upon the District's request, provide the District with a copy of its response.

6.2 Received by District. If the District receives a subpoena, warrant, or other legal order, demand or request seeking District Data maintained by Contractor, the District will promptly notify Contractor and, within two (2) business days, excluding national holidays, Contractor shall supply the District with copies of the District Data for the District to respond. If the requested data is so large that it cannot be reasonably compiled and provided within 2 days, the Contractor shall inform the District of the reasons why the data cannot be compiled and provided within 2 days and how long it will take under reasonable conditions and at what cost to the District.

6.3 Parent Request. If a parent, legal guardian or student contacts the District with a request to review or correct District Data or PII, pursuant to FERPA, the District will promptly notify Contractor's Designated Representative and Contractor shall use reasonable and good faith efforts to assist the District in fulfilling such requests, as directed by the District, within ten calendar (10) days after receipt of District's notice with standard fees applied. Conversely, if a parent, legal guardian or student contacts the Contractor with a request to review or correct District Data or PII, within ten calendar (10) days after receipt of such notice, Contractor

shall promptly notify the District and shall use reasonable and good faith efforts to assist the District in fulfilling such requests, as directed by the District.

6.4 Access to District Data. District shall have the right to access and retrieve any or all District Data stored by or in possession of Contractor upon written notice to Contractor's Designated Representative. If another timeline for response is provided herein, then that, more specific, deadline shall control. Otherwise, Contractor shall make the District Data available to the District within seven (7) calendar days from the date of request.

7. Compliance with Applicable Law

7.1 School Service Contract Providers. If Contractor provides a "school service," which is defined as an Internet website, online service, online application or mobile application that: (a) is designed and marketed primarily for use in a preschool, elementary school or secondary school; (b) is used at the direction of District teachers or other District employees; and (c) collects, maintains or uses District Data or PII, then Contractor is a "school service contract provider" under the Act. To the extent not previously provided, within ten (10) calendar days after signing this Addendum, Contractor shall provide to the District in a format acceptable to the District or that is easily accessible through Contractor's website in language easily understandable to a layperson: (a) the data elements of District Data or PII that Contractor collects, generates or uses pursuant to the Contract; (b) the educational purpose for which Contractor collects and uses the District Data; (c) Contractor's policies regarding retention and disposal of District Data; (d) how Contractor uses, shares or discloses the District Data; and (e) statement whether Contractor's Contract has ever been terminated by another school district for failure to comply with the same or substantially similar security obligations as those set forth herein. Contractor shall update this information as necessary to maintain accuracy. District reserves the right to terminate this Agreement, as specified in Section 8, should the District receive information after the Effective Date that significantly modifies Contractor's representations made in this Section 7.1.

7.2. Children's Online Privacy and Protection Act. In performance of the Services required by the Contract, if Contractor collects personal information (as defined in the Children's Online Privacy and Protection Act of 1998, 5 U.S.C. 6501 to 6505, and its implementing regulations) from children under thirteen (13) years of age, Contractor warrants, represents, and covenants that such collection is and shall be for the use and benefit of the District and for no other commercial purpose. Contractor has provided District with full notice of its collection, use, and disclosure practices.

7.3 Compliance with Laws. Contractor warrants that it will abide by all applicable laws, ordinances, rules, regulations, and orders of all governmental agencies or authorities having jurisdiction over the Services including but not limited to: COPPA; FERPA; the Health Insurance Portability and Accountability Act, 45 C.F.R. Part 160.103, and Health Information Technology for Economic and Clinical Health Act, Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. 6809; Payment Card Industry Data Security Standards; Protection of Pupil Rights Amendment, 20 U.S.C. 1232h, 34 C.F.R. Part 98; Americans with Disabilities Act, and Federal Export Administration Regulations.

8. Termination

8.1 Term. This Addendum will become effective when the Contractor has executed this Addendum ("Effective Date"). Subject to Sections 8.2 and 12.3, this Addendum will automatically terminate without any further action of the Parties upon the termination or expiration of the Contract between the Parties or successful completion of the Services. Alternatively, upon re-execution of the Contract by the authorized persons of District and Contractor, this Addendum shall also be revived and be of full force and effect.

8.2 Termination by the District.

8.2.1 The District may immediately terminate the Contract in accordance with District policies if, at any time, the District determines in its sole discretion, that Contractor has breached any of the requirements of this Addendum.

8.2.2 The District may terminate the Contract if District receives information that Contractor has failed to comply with the same or substantially similar security obligations as set forth herein with another

school district.

8.2.3 The District may terminate the Contract if the District receives information after execution of this Addendum, that any of Contractor's representations or warranties have substantially changed after execution of this Addendum, including but not limited to the terms of Contractor's privacy policy.

9. Data Transfer Upon Termination or Expiration

9.1 Destruction or Return of District Data. With the exception of De-identified Data that District has specifically agreed in writing to allow Contractor to use after termination or expiration of this Agreement, or District Data for which Contractor has specifically obtained consent from the parent, legal guardian or student to keep, within thirty (30) calendar days after termination or expiration of this Agreement, Contractor shall ensure that all District Data and PII that Contractor collected, generated or inferred pursuant to the Contract ("Contract Data"), is securely returned or Securely Destroyed, as directed by the District. In the event that the District requests destruction, Contractor agrees to Securely Destroy all District Data and Contract Data that is in its possession and cause its Subcontractors to Securely Destroy all District Data and Contract Data that is in the possession of any Subcontractors. If the District requests return, Contractor shall securely return all District Data and Contract Data to the authorized person specified by the District, using the methods requested by the District, in its discretion, including any applicable fees charged to the District by the Contractor. The Contractor shall promptly certify in writing to District that such District Data and Contract Data has been disposed of or returned securely.

9.2 Transfer and Destruction of District Data. If the District elects to have all District Data or Contract Data that is in Contractor's possession or in the possession of Contractor's Subcontractors transferred to a third party designated by the District, such transfer shall occur within a reasonable period of time but no later than thirty (30) calendar days after expiration or termination of this Agreement, and without significant interruption in service or access to such District Data. Contractor shall work closely with such third party transferee to ensure that such transfer/migration uses facilities and methods are compatible with the relevant systems of the District or its transferee, and to the extent technologically feasible, that the District will have reasonable access to District Data during the transition. District will pay all costs associated with such transfer, unless such transfer is as the result of termination of this Agreement following Contractor's breach of the terms of this Agreement. Upon successful transfer of District Data, as confirmed in writing by the District's Designated Representative, Contractor shall Securely Destroy all District Data in accordance with Section 9.1.

9.3 Response to Specific Data Destruction or Return Requests. Contractor shall Securely Destroy or return any specific District Data or Contract Data that is in its possession or in the possession of its Subcontractors within five (5) business days, excluding national holidays, after receiving a written request from the District.

10. Indemnification

Contractor shall indemnify and hold harmless District and its directors, employees, board members and agents from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, award, penalties, fines, costs or expenses, including attorneys' fees, the costs of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers, arising out of or resulting from any third-party claim against District or its directors, employees, board members and agents arising out of or resulting from Contractor's failure to comply with any of its obligations under Sections 3, 4, 5, and 9 of this Addendum. These indemnification duties shall survive termination or expiration of this Agreement.

11. Miscellaneous

11.1 No End User Agreements. In the event that the Contractor enters into terms of use agreements or other agreements or understandings, whether electronic, click-through, verbal or in writing, with End Users, the parties agree that in the event of a conflict between the terms of any such agreement and this Addendum, the terms of this Addendum and the Agreement, in that order of precedence, shall control.

11.2 Public Inspection of Agreement. Contractor acknowledges and agrees that this Agreement and all documents Contractor provides District as required herein, are public records for purposes of SOPPA and shall at all times be subject to public inspection.

11.3 Survival. The Contractor's obligations under Sections 3, 4, 5, 6, 9, and 10, and any other obligations or

restrictions that expressly or by their nature are to continue after termination, shall survive termination of this Agreement for any reason until all District Data has been returned or Securely Destroyed.

11.4 Governing Law. This Addendum shall be governed and construed in accordance with the laws of Illinois, excluding its choice of law rules. In performing their respective obligations under the Agreement, both parties shall comply with all Illinois laws and regulations pertaining to student data privacy and confidentiality, including but not limited to the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 70 ILCS 110/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/.

11.5 No Assignment. Contractor shall not assign or subcontract any of its rights or obligations hereunder without the express written consent of District, which will not be unreasonably withheld.

11.6 No Third Party Beneficiaries. Nothing in this Agreement shall be construed to give any rights or benefits to anyone other than District.

11.7 Schedules. The following schedules are attached hereto, or shall be attached hereto, and are specifically made a part hereof by this reference:

Schedule 1 -- Designated Representatives
Schedule 2 -- Subcontractors

11.8 Counterparts. This Addendum may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

SCHEDULE 1
District/Contractor Designated Representative

DISTRICT REPRESENTATIVE	CONTRACTOR REPRESENTATIVE
Name: Douglas J. Kahler Title: Director of Information Services Address: 1 Stevenson Drive Lincolnshire, IL 60069 Phone: 847.415.4301 E-mail: dkahler@d125.org	Name: Steven K. Bohlender Title: Executive Vice President Address: 2843 31st Avenue Greeley, CO 80631 Phone: 800.437.7457 x-123 E-mail: sbohlender@cicesp.com

SCHEDULE 2
Subcontractors

Contractor shall update this information as necessary to maintain accuracy and shall send revised attachments, exhibits or schedules to the District's Authorized Representative.

Name of Subcontractor	Not applicable - none
Primary Contact Person	
Subcontractor Address	
Subcontractor Phone/email	
Purpose of re-disclosure to Subcontractor	

COMPUTER INFORMATION CONCEPTS, INC.

By: Steven K. Bohlender

Name: Steven K. Bohlender

Date: Jan 11, 2022

CUSTOMER

By: Douglas J Kahler
Douglas J Kahler (Jan 11, 2022 12:17 CST)

Name: Douglas J Kahler

Date: Jan 11, 2022