Addendum D

SULLIVAN BOCE PARENTS Bill of RIGHTS for Data Privacy and Security

The District will publish its Parents' Bill of Rights for Data Privacy and Security (Bill of Rights) on its website. Additionally, the District will include the Bill of Rights with every contract or other written agreement it enters into with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from the District.

The District's Bill of Rights will state in clear and plain English terms that:

a. A student's personal identifiable information (PII) cannot be sold or released for any commercial purposes;

b. Parents have the right to inspect and review the complete contents of their child's education record;

c. State and federal laws protect the confidentiality of PII, 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;

d. A complete list of all student data elements collected by the state is available for public review at the following website http://www.nysed.gov/student-data-privacy/student-data-inventory or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234; and

e. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, 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/student-data-privacy/form/report-improper-disclosure. Parents can also send their written complaint to the Sullivan BOCES Data Protection Officer at 15 Sullivan Avenue, Suite 1, Liberty New York 12754

Addendum E

PARENTS' BILL OF RIGHTS - SUPPLEMENTAL INFORMATION ADDENDUM

1. **EXCLUSIVE PURPOSES FOR DATA USE:** The exclusive purposes for which "student data" or "teacher or principal data" (as those terms are defined in Education Law Section 2-d and collectively referred to as the "Confidential Data") will be used by I-CAR **(the "Vendor")** are limited to the purposes authorized in the contract between the Vendor and Sullivan County BOCES **(the "BOCES")** dated _____ **(the "Contract Date")**.

2. **SUBCONTRACTOR OVERSIGHT DETAILS:** The Vendor will ensure that any subcontractors, or other authorized persons or entities to whom the Vendor will disclose the Confidential Data, if any, are contractually required to abide by all applicable data protection and security requirements, including but not limited to, those outlined in applicable State and Federal laws and regulations (e.g., Family Educational Rights and Privacy Act ("FERPA"); Education Law § 2-d; 8 NYCRR § 121).

3. **CONTRACT PRACTICES:** The Contract commences and expires on the dates set forth in the Contract unless earlier terminated or renewed pursuant to the terms of the Contract. On or before the date the Contract expires, protected data will be exported to the BOCES in: (choose one)

☐ The agreed upon format to BOCES unless otherwise directed by BOCES or the student whose protected data it is(or)

☐ W[illegible]be destroyed by the Vendor as directed by the BOCES

4. **DATA ACCURACY/CORRECTION PRACTICES:** A parent or eligible student can challenge the accuracy of any "education record", as that term is defined in the FERPA, stored by the BOCES in a

Vendor's product and/or service by following the BOCES's procedure for requesting the amendment of education records under the FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by BOCES in the Vendor's product and/or service by following the appeal

procedure in the BOCES's APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.

5. **SECURITY PRACTICES:** Confidential Data provided to the Vendor by the BOCES will be stored in the United States. The measures that the Vendor takes to protect Confidential Data will align with the

NIST Cybersecurity Framework, including but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

6. **ENCRYPTION PRACTICES:** The Vendor will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section 2-d and other applicable law.

Addendum F

VENDOR'S INFORMATION PROTECTION, SECURITY and PRIVACY GUIDELINES

I-CAR Information Protection, Security and Privacy Guidelines

This Information Protection, Security and Privacy Document sets forth specific standards by I-CAR (as defined below) concerning the protection, security, and privacy of the information of I-CAR education segment (Users) which I-CAR may receive or have access to in the course of I-CAR's performance of services for Users.

Definitions:

"User" means any person within the educational segment that utilizes I-CAR services.

"Patches" shall mean software update code provided by specific vendors to correct an identified vulnerability within Software or on I-CAR's system, computer, network, or other equipment.

"Personal Data" means any information relating to a User, as provided by the User for purposes of accessing I-CAR's services.

"User Information" means any User Records or proprietary data of User in possession of, or accessible by, ICAR.

"I-CAR" means the entity which contracts to provide products to User under the Agreement.

"Cryptography" is the discipline that embodies the principles, means, and methods for providing information security, including confidentiality, data integrity, and non-repudiation.

"Malicious" Code" means any computer instructions in Software that are not intended to provide the functionality described in the Software specifications and that interfere with User's right to quiet enjoyment

of its license to the Software (as applicable) or its information systems or that interfere with or prevent User use of the Software or its information systems as contemplated in the Agreement. Malicious Code includes without limitation such computer instructions commonly known as computer viruses, "Trojan horses," anomalies, self-destruction mechanisms, copy protection bypass schemes, and any other computer instructions that interfere with or prevent User from using the User Information or Software as described in its specifications or as contemplated in the Agreement. Malicious Code also includes without limitation any computer instructions that can: (i) disable, destroy, or otherwise alter the User Information or any hardware on which the Software executes; or (ii) reveal any data or other information accessed through or processed by the Software to anyone outside of User without User's knowledge and prior approval.

"Patches" shall mean software update code provided by specific vendors to correct an identified vulnerability within Software or on I-CAR's system, computer, network, or other equipment.

"Personal Data" means any information relating to a User, as provided by the User for purposes of accessing I-CAR's services.

"Privacy Laws" means all federal, state, and local U.S. laws and rules relating to Personal Data and other data privacy and data protection, as they may be enacted.
"Processing of (or to Process) Personal Data" means any operation or set of functions that is performed upon Personal Data and includes, without limitation, the following: access, collection, use, retention, copying, recording, organization, storage, adaptation or alteration, enriching, retrieval, transmission, dissemination or otherwise making available, and disposal or destruction of Personal Data.

"Security Breach" means any Security Incident in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so.

"Security Incident" means the confirmed unauthorized access to Users information that was intended to or reasonably likely to compromise Users information, network, computer systems, or Software. Security Incidents include, but are not limited to, information system failures and loss of service, denial of service, errors resulting from incomplete or inaccurate business data, and confidentiality breaches. Security Incidents will be considered confidential.

"Security Vulnerability" means a weakness at the network services, operating system, or application level,

or within associated functions of networks, computer systems, or Software that could allow a Security Incident to occur.

2.0 KEY SECURITY REQUIREMENTS

2.1 Information Systems. I-CAR has implemented and maintains information systems that are reasonably suitable to protect the security of User's information processed, including, without limitation, physical, network, host, web, and data security.

2.2 Security Measures. I-CAR will maintain security precautions consistent with current industry standards and best practices.

2.3 Privacy Laws. Any Personal Data Processed by the I-CAR while performing its services under the Agreement will be processed, protected, and deleted per all applicable Privacy Laws.
2.4 Breach Notification. I-CAR will inform User promptly in writing of the occurrence of any Security Breach involving or related to information of the User, provided User has given I-CAR correct contact information (e-mail).

3.0 PROTECTION OF SYSTEMS AND INFORMATION

3.1 Security Vulnerabilities

3.1.1 Vulnerabilities. I-CAR has implemented a security vulnerability management program for all systems, computers, networks, applications, or other computer equipment used in support of User.

3.1.2 Vulnerability Classification. I-CAR has classified Security Vulnerabilities using industry- recognized standards.

3.1.3 Vulnerability Correction. I-CAR will use patches and other Software and hardware updates Code to correct all identified vulnerabilities on systems, computers, networks, applications, or other computer equipment. The I-CAR will address and remediate security vulnerabilities within a reasonable time frame within industry standards.

3.1.4 Malware Response. I-CAR will maintain a documented process for responding to malware outbreaks.

3.1.5 Denial of Service. I-CAR has implemented appropriate safeguards to protect against or limit the effects of Denial-of-Service attacks and will monitor to detect indicators of denial of service attacks against information systems that process or store User Information.

3.2 Users

3.2.1 General. I-CAR has implemented the following rules for I-CAR Users who access systems that store or process User Information.

3.2.2 I-CAR User Accounts

a. Each I-CAR User will be assigned a unique account identifier or User ID. No anonymous logins will be permitted.
b. User IDs must not be shared or used by anyone other than the User to whom it was assigned. Users are accountable for all activity associated with their User IDs.
c. User IDs must be added, modified, and deleted in accordance with I-CAR approved account management processes.
d. Only I-CAR Users with a business need-to-know are to be provided with passwords, accounts, or keys for access to User Information.
e. All systems must limit the number of failed log-on attempts before disabling the User ID.

3.2.3 Logging

a. All systems must limit the number of failed log-on attempts to three (3) before disabling the User ID.

4.0 Encryption and Retention of User Information

4.1 Encryption – Transmission

I-CAR utilizes known secure Cryptography to protect User information in transit.

4.1 Encryption – Storage

I-CAR will protect all copies of User Information at rest using known secure Cryptography.

4.2 Retention and Disposal

I-CAR will cooperate with User in deleting User information if requested.

5.0 INCIDENT RESPONSE

5.1 General. I-CAR will adhere to the following guidelines in the event of an incident affecting User Information.

5.2 Notification

5.2.1 Initial Notification of Security Incident. I-CAR shall notify the User of any relevant data security incidents by way of the Incident Response Team.

5.3 Communications. I-CAR shall notify User via e-mail and in writing of any security incidents relevant to User information.

6.0 SPECIFIC SECURITY REQUIREMENTS

6.1 Software Support. I-CAR will be fully responsible for implementing and maintaining reasonable security measures to ensure that any software updates provided to User are free of malicious Code and that all updates are provided securely to be agreed upon by both parties.

6.2 Hyperlinks and Websites. I-CAR provides reasonable security measures to protect hyperlinks that reference User websites.