Addendum A

CiTi BOCES PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Parents (includes legal guardians or persons in parental relationships) and Eligible Students (student 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as defined by Education Law § 2-d and FERPA, includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including but not limited to encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at

http://www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. Complaints may be submitted to NYSED at http://www.nysed.gov/data-privacy-security/report-improper-disclosure , by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474- 0937. Complaints regarding student data breaches can also be directed to: Kristen Foland, Director of Instructional Support Services, Center for Instruction, Technology & Innovation, 179 County Route 64, Mexico NY, 13114. Phone: 315-963-4425 email: kfoland@citiboces.org.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII

occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

Addendum B

PARENTS' BILL OF RIGHTS – SUPPLEMENTAL INFORMATION ADDENDUM

1. As used in this Addendum B, the following terms will have the following meanings:

a. "Student" shall have the meaning defined in Subsection 1(f) of Section 2-d.

b. "Eligible Student" shall have the meaning defined in Subsection 1(g) of Section 2-d.

c. "Personally Identifiable Information" as applied to Student Data shall have the meaning defined in Subsection 1(d) of Section 2-d.

d. "Student Data" means Personally Identifiable Information from student records that Vendor receives from CiTi BOCES.

Other capitalized terms used in this Addendum B will have the applicable meaning set forth elsewhere in this Agreement or in Section 2-d.

2. Vendor agrees that the confidentiality of Student Data shall be maintained in accordance with state and federal laws that protect the confidentiality of Student Data.

3. Vendor agrees that any of its officers or employees, and any officers or employees of any assignee of Vendor, who have access to Student Data will be provided training on the federal and state law governing confidentiality of such Student Data prior to receiving access to that data.

4. The exclusive purpose for which Vendor is being provided access to Student Data is to permit Vendor to provide Services as set forth in the Agreement. Student Data received by Vendor, or by any assignee of Vendor or third party contracting with Vendor, shall not be sold or used for marketing purposes.

5. If Vendor comes into possession of Student Data, Vendor will only share such Student Data with additional third parties if those third parties are contractually bound to adhere to 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 Part 121).

6. 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 CiTi BOCES in [insert data format] format and/or destroyed by the Contractor as directed by CiTi BOCES.

7. If a parent, Student, or Eligible Student wishes to challenge the accuracy of any "education record", as that term is defined in the FERPA, by following the School District'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 CiTi BOCES in Contractor's product and/or service by following the appeal procedure in the School District's APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.

8. Student Data transferred to Vendor by CiTi BOCES will be stored in electronic memory (on servers or other computers) operated and maintained by or on behalf of Vendor in the United States. The measures that Vendor will take to protect the privacy and security of Student Data while it is stored in that manner include, but are not necessarily limited to: encryption to the extent required by Section 2-d; restricted physical access to the servers/computers; software-based solutions intended to prohibit unauthorized entry such as regularly updated virus scans, firewalls, and use of passwords; and administrative controls such as selective user access rights. The measures that Vendor takes to protect Confidential Data will align with the NIST Cybersecurity Framework.

9. The Contractor 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.