SCHEDULE C-1

[Signed copy of Southern Westchester BOCES Parent Bill of Rights]

Parents' Bill of Rights for Data Privacy and Security

In accordance with New York State Education Law Section 2-d, the Southern Westchester Board of Cooperative Educational Services ("Southern Westchester BOCES") hereby sets forth the following Parents' Bill of Rights for Data Privacy and Security, which is applicable to all students and their parents and legal guardians.

(1) New York Stated Education law Section 2-d (Section 2-d") and the Family Educational Rights and Privacy Act ("FERPA") protect the confidentiality of personally identifiable information. Section 2-d and FERPA assure the confidentiality of records with respect to "third parties," and provides parents with the right to consent to disclosures of personally identifiable information contained in their child's education records. Exceptions to this include school employees, officials and certain State and Federal officials who have a legitimate educational need to access such records. In additions, the Southern Westchester BOCES will, upon request of parents, legal guardians or eligible students, or if otherwise required by law, disclose student records to officials of another school district in which a student seeks to enroll. An eligible student is a student who has reached 18 years of age or attends a postsecondary institution.

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

(3) Personally, identifiable information includes, but is not limited to:

i. The student's name;

ii. The name of the student's parent or other family members;

iii. The address of the student or student's family;

iv. A personal identifier, such as the student's social security number, student number, or biometric record;

v. Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;

vi. Other information that, alone or in combination, is linked or linkable to a specific student that would 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; or

vii. Information requested by a person who the Southern Westchester BOCES reasonably believes knows the identity of the student to whom the education record relates.

(4) In accordance with FERPA, Section 2-d and Southern Westchester BOCES Policy No. 6320, Student Records: Access and Challenge, parents and legal guardians have the right to inspect and review the complete contents of their child's education record.

(5) Southern Westchester BOCES has the following safeguards in place: Encryption, firewalls and password protection, which must be in place when data is stored or transferred.

(6) New York State, through the New York State Education Department, collects a number of student data elements for authorized uses. A complete list of all student data elements collected by the State is available for public review at the following links or can be obtained by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, NY 12234:

http://www.p12.nysed.gov/irs/data_reporting.html
http://data.nysed.gov/
http://www.p12.nysed.gov/irs/sirs/documentation/nyssisguide.pdf

(7) Eligible students, parents and legal guardians have the right to have complaints about possible breaches of student data addressed. Any such complaint should be submitted, in writing, to the Data Protection Officer of Southern Westchester BOCES at dpo@swboces.org or at 450 Mamaroneck Avenue, Harrison, New Yorkk 10528. Parents can direct any complaints regarding possible breaches via the electronic form on the Southern Westchester BOCES home page, under Resources, and Student Privacy. The complaint form can also be found by going to https://bit.ly/swbdatabreach. Alternatively, a written complaint may also be submitted to the Chief Privacy Officer of the New York State Education Department using the form available at http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure or writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234.

Supplemental Information for Agreement with Emics, Inc. dba Informed K12 (hereinafter "Company")

(1) The personally identifiable student data or teacher or principal data (collectively, "the Data") received by Company will be used exclusively for the following purpose(s):
The Informed K12 platform provides a workflow automation and esignature tool for any forms Customers choose to put on line. The platform will host data purely for the use of the districts or schools use. The Company does not use data entered into the form directly for any marketing or commercial purpose; the data is only accessed in the normal course of servicing the Customer.

(2) The Company will ensure that all subcontractors and other authorized persons or entities to whom Data will be disclosed will abide by all applicable data protection and security requirements, including those mandated by New York State and federal laws and regulations, by the following means:
All employees undergo data security and privacy training within their first 30 days at the Company and annually thereafter. Subcontractor contracts are reviewed for access to data and, if there is access to data, for protocols that abide by all contractual agreements.

(3) The Agreement with Company commenced on _June 22, 2022_____. The initial term ends on June 30, 2023_; however, the term is automatically renewed for 12 month periods unless Company or Southern Westchester BOCES provide notice of non-renewal at least thirty days prior to the expiration of the applicable term. Upon the expiration or termination of the Agreement, all Data will be (check all that apply and fill in required information):

☐ Returned to Customers by _____ [date] in the following format(s):_____

_____

☐ Returned to Southern Westchester BOCES by _____ [date] in the following format(s): _____

_____

X Securely destroyed by 30 days after the termination date in the following manner:

Customers are responsible for downloading any form data they need to retain; the platform provides the capability for form managers and owners to download data in bulk for each form. All platform data will be securely destroyed and no longer retrievable at the conclusion of the data retention period.

☐ Other – explain _____

_____

_____

☐ If student data or teacher or principal data is to be maintained by Company for any lawful purpose, such data shall remain in an encrypted format and shall be stored on systems maintained by Company in a secure data facility located within the United States.

(4) In the event that a student's parent or guardian or an eligible student seeks to challenge the accuracy of student data pertaining to the particular student, which data may include records maintained, stored, transmitted or generated by the Third-party Contractor pursuant to its Agreement with Southern Westchester BOCES, the challenge will be directed to Southern Westchester BOCES and processed in accordance with the procedures of Southern Westchester BOCES. In the event that a teacher or principal seeks to challenge the accuracy of teacher or principal data pertaining to the particular teacher or principal, which data may include records maintained, stored, transmitted or generated by the Third-party Contractor pursuant to its Agreement with Southern Westchester BOCES, the challenge will be directed to Southern Westchester BOCES and processed in accordance with the procedures Southern Westchester BOCES has established for challenging annual professional performance review ("APPR") data.

(5) Describe where the Data will be stored (in a manner that will protect data security) and the security protections that will be taken by Company to ensure the Data will be protected and data security and privacy risks mitigated:

Informed K12's platform data is stored in the "Heroku Postgres" database system. Under that system, customer data is stored in separate access-controlled databases per application. Each database requires a unique username and password that is only valid for that specific database and is unique to a single application. Customers with multiple applications and databases are assigned separate databases and accounts per application to mitigate the risk of unauthorized access between applications. Customer connections to postgres databases require SSL encryption to ensure a high level of security and privacy.

(6) Describe how the Data will be protected using encryption while in motion and at rest:

Data center providers used by Informed K12 offer both encryption-at-rest and Continuous Protection which helps keep data safe by archiving new data every 60 seconds and performing 20 diagnostics health checks every 30 seconds. If a diagnostic should fail, then automated systems repair the database automatically. Important business data stored in the databases is recoverable. With encryption-at-rest, in the exceedingly unlikely event of a physical breach of their underlying infrastructure (i.e., if someone broke into the datacenter and removed the disk drives), they would still not gain access to the database unless they also had all encryption keys and credentials.

Company Name: Emics, Inc.

Authorized Signature: 

Authorized Signer's Name & Title: Sarah Chou, CEO

Date: 6/17/22