Appendix S: PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

To satisfy their responsibilities regarding the provision of education to students in pre-kindergarten through grade twelve, "educational agencies" (as defined below) in the State of New York collect and maintain certain personally identifiable information from the education records of their students. As part of the Common Core Implementation Reform Act, Education Law §2-d requires that each educational agency in the State of New York must develop a Parents' Bill of Rights for Data Privacy and Security (Parents' Bill of Rights). The Parents' Bill of Rights must be published on the website of each educational agency, and must be included with every contract the educational agency enters into with a "third party contractor" (as defined below) where the third party contractor receives student data, or certain protected teacher/principal data related to Annual Professional Performance Reviews that is designated as confidential pursuant to Education Law §3012-c ("APPR data").

The purpose of the Parents' Bill of Rights is to inform parents (which also include legal guardians or persons in parental relation to a student, but generally not the parents of a student who is age eighteen or over) of the legal requirements regarding privacy, security and use of student data. In addition to the federal Family Educational Rights and Privacy Act (FERPA), Education Law §2-d provides important new protections for student data, and new remedies for breaches of the responsibility to maintain the security and confidentiality of such data.

A. What are the essential parents' rights under the Family Educational Rights and Privacy Act (FERPA) relating to personally identifiable information in their child's student records?

The rights of parents under FERPA are summarized in the Model Notification of Rights prepared by the United States Department of Education for use by schools in providing annual notification of rights to parents. It can be accessed at http://www2.ed.gov/policy/gen/guid/fpco/ferpa/lea-officials.html, and a copy is attached to this Parents' Bill of Rights. Complete student records are maintained by schools and school districts, and not at the New York State Education Department (NYSED). Further, NYSED would need to establish and implement a means to verify a parent's identity and right of access to records before processing a request for records to the school or school district. Therefore, requests to access student records will be most efficiently managed at the school or school district level.

Parents' rights under FERPA include:

1. The right to inspect and review the student's education records within 45 days after the day the school or school district receives a request for access.

2. The right to request amendment of the student's education records that the parent or eligible student believes are inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA. Complete student records are maintained by schools and school districts and not at NYSED, which is the secondary repository of data, and NYSED make amendments to school or school district records. Schools and school districts are in the best position to make corrections to students' education records.

3. The right to provide written consent before the school discloses personally identifiable information (PII) from the student's education records, except to the extent that FERPA authorizes disclosure without consent (including but not limited to disclosure under specified conditions to: (i) school officials within the school or school district with legitimate educational interests; (ii) officials of another school for purposes of enrollment or transfer;

(iii) third party contractors providing services to, or performing functions for an educational agency; (iv) authorized representatives of the U. S. Comptroller General, the U. S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as NYSED; (iv) (v) organizations conducting studies for or on behalf of educational agencies) and (vi) the public where the school or school district has designated certain student data as "directory information" (described below). The attached FERPA Model Notification of Rights more fully describes the exceptions to the consent requirement under FERPA).

4. Where a school or school district has a policy of releasing "directory information" from student records, the parent has a right to refuse to let the school or school district designate any all of such information as directory information. Directory information, as defined in federal regulations, includes: the student's name, address, telephone number, email address, photograph, date and place of birth, major field of study, grade level, enrollment status, dates of attendance, participation in officially recognized activities and sports, weight and height of members of athletic teams, degrees, honors and awards received and the most recent educational agency or institution attended. Where disclosure without consent is otherwise authorized under FERPA, however, a parent's refusal to permit disclosure of directory information does not prevent disclosure pursuant to such separate authorization.

5. The right to file a complaint with the U.S. Department of Education concerning alleged failures by the School to comply with the requirements of FERPA.

B. What are parents' rights under the Personal Privacy Protection Law (PPPL), Article 6-A of the Public Officers Law relating to records held by State agencies?

The PPPL (Public Officers Law §§91-99) applies to all records of State agencies and is not specific to student records or to parents. It does not apply to school districts or other local educational agencies. It imposes duties on State agencies to have procedures in place to protect from disclosure of "personal information," defined as information which because of a name, number, symbol, mark or other identifier, can be used to identify a "data subject" (in this case the student or the student's parent). Like FERPA, the PPPL confers a right on the data subject (student or the student's parent) to access to State agency records relating to them and requires State agencies to have procedures for correction or amendment of records.

A more detailed description of the PPPL is available from the Committee on Open Government of the New York Department of State. Guidance on what you should know about the PPPL can be accessed at http://www.dos.ny.gov/coog/shldno1.html. The Committee on Open Government's address is Committee on Open Government, Department of State, One Commerce Plaza, 99 Washington Avenue, suite 650, Albany, NY 12231, their email address is coog@dos.ny.gov, and their telephone number is (518) 474-2518.

C. Parents' Rights Under Education Law §2-d relating to Unauthorized Release of Personally Identifiable Information

1. What "educational agencies" are included in the requirements of Education Law §2-d?

- The New York State Education Department ("NYSED");
- Each public-school district;
- Each Board of Cooperative Educational Services or BOCES; and

- All schools that are:
  - a public elementary or secondary school;
  - a universal pre-kindergarten program authorized pursuant to Education Law §3602-e;
  - an approved provider of preschool special education services;
  - any other publicly funded pre-kindergarten program;
  - a school serving children in a special act school district as defined in Education Law 4001; or
  - certain schools for the education of students with disabilities - an approved private school, a state-supported school subject to the provisions of Education Law Article 85, or a state-operated school subject to Education Law Article 87 or 88.

2. What kind of student data is subject to the confidentiality and security requirements of Education Law §2-d?

The law applies to personally identifiable information contained in student records of an educational agency listed above. The term "student" refers to any person attending or seeking to enroll in an educational agency, and the term "personally identifiable information" ("PII") uses the definition provided in FERPA. Under FERPA, personally identifiable information or PII 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 of the student or student's family;
(d) A personal identifier, such as the student's social security number, student number, or biometric record;
(e) Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name[1];
(f) 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
(g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

3. What kind of student data is *not* subject to the confidentiality and security requirements of Education Law §2-d?

The confidentiality and privacy provisions of Education Law §2-d and FERPA extend only to PII, and not to student data that is not personally identifiable. Therefore, de-identified data (e.g., data regarding students that uses random identifiers), aggregated data (e.g., data reported at the school district level) or anonymized data that could not be used to identify a particular student is not considered to be PII and is not within the purview of Education Law §2-d or within the scope of this Parents' Bill of Rights.

4. What are my rights under Education Law § 2-d as a parent regarding my student's PII?

[1] Please note that NYSED does not collect certain information defined in FERPA, such as students' social security numbers, biometric records, mother's maiden name (unless used as the mother's legal name).

Education Law §2-d ensures that, in addition to all of the protections and rights of parents under the federal FERPA law, certain rights will also be provided under the Education Law. These rights include, but are not limited to, the following elements:

(A) A student's PII cannot be sold or released by the educational agency for any commercial or marketing purposes.

o PII may be used for purposes of a contract that provides payment to a vendor for providing services to an educational agency as permitted by law.

o However, sale of PII to a third party solely for commercial purposes or receipt of payment by an educational agency, or disclosure of PII that is not related to a service being provided to the educational agency, is strictly prohibited.

(B) Parents have the right to inspect and review the complete contents of their child's education record including any student data stored or maintained by an educational agency.

- This right of inspection is consistent with the requirements of FERPA. In addition to the right of inspection of the educational record, Education Law §2-d provides a specific right for parents to inspect or receive copies of any data in the student's educational record.
- NYSED will develop policies for annual notification by educational agencies to parents regarding the right to request student data. Such policies will specify a reasonable time for the educational agency to comply with such requests.
- The policies will also require security measures when providing student data to parents, to ensure that only authorized individuals receive such data. A parent may be asked for information or verifications reasonably necessary to ensure that he or she is in fact the student's parent and is authorized to receive such information pursuant to law.

(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.

Education Law §2-d also specifically provides certain limitations on the collection of data by educational agencies, including, but not limited to:

(A) A mandate that, except as otherwise specifically authorized by law, NYSED shall only collect PII relating to an educational purpose;

(B) NYSED may only require districts to submit PII, including data on disability status and student suspensions, where such release is required by law or otherwise authorized under FERPA and/or the New York State Personal Privacy Law; and

(C) Except as required by law or in the case of educational enrollment data, school districts shall not report to NYSED student data regarding juvenile delinquency records, criminal records, medical and health records or student biometric information.

(D) Parents may access the NYSED Student Data Elements List, a complete list of all student data elements collected by NYSED, at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, or may obtain a copy of this list by writing to the Office of Information & Reporting Services,

New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234; and

(E) Parents have the right to file complaints with an educational agency about possible breaches of student data by that educational agency's third-party contractors or their employees, officers, or assignees, or with NYSED. Complaints to NYSED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email to CPO@mail.nysed.gov. The complaint process is under development and will be established through regulations to be proposed by NYSED's Chief Privacy Officer, who has not yet been appointed.

o Specifically, the Commissioner of Education, after consultation with the Chief Privacy Officer, will promulgate regulations establishing procedures for the submission of complaints from parents, classroom teachers or building principals, or other staff of an educational agency, making allegations of improper disclosure of student data and/or teacher or principal APPR data by a third-party contractor or its officers, employees or assignees.

o When appointed, the Chief Privacy Officer of NYSED will also provide a procedure within NYSED whereby parents, students, teachers, superintendents, school board members, principals, and other persons or entities may request information pertaining to student data or teacher or principal APPR data in a timely and efficient manner.

5. Must additional elements be included in the Parents' Bill of Rights.?

Yes**.** For purposes of further ensuring confidentiality and security of student data, as an appendix to the Parents' Bill of Rights each contract an educational agency enters into with a third-party contractor shall include the following supplemental information:

(A) the exclusive purposes for which the student data, or teacher or principal data, will be used;

(B) how the third-party contractor will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

(C) when the agreement with the third-party contractor expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

(D) if and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

(E) where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

a. In addition, the Chief Privacy Officer, with input from parents and other education and expert stakeholders, is required to develop additional elements of the Parents' Bill of Rights to be prescribed in Regulations of the Commissioner.

6. What protections are required to be in place if an educational agency contracts with a third-party contractor to provide services, and the contract requires the disclosure of PII to the third-party contractor?

Education Law §2-d provides very specific protections for contracts with "third party contractors", defined as any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency. The term "third party contractor" also includes an educational partnership organization that receives student and/or teacher or principal APPR data from a school district to carry out its responsibilities pursuant to Education Law §211-e, and a not-for-profit corporation or other non-profit organization, which are not themselves covered by the definition of an "educational agency."

Services of a third-party contractor covered under Education Law §2-d include, but not limited to, data management or storage services, conducting studies for or on behalf of the educational agency, or audit or evaluation of publicly funded programs.

When an educational agency enters into a contract with a third-party contractor, under which the third-party contractor will receive student data, the contract or agreement must include a data security and privacy plan that outlines how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the educational agency's policy on data security and privacy. However, the standards for an educational agency's policy on data security and privacy must be prescribed in Regulations of the Commissioner that have not yet been promulgated. A signed copy of the Parents' Bill of Rights must be included, as well as a requirement that any officers or employees of the third-party contractor and its assignees who have access to student data or teacher or principal data have received or will receive training on the federal and state law governing confidentiality of such data prior to receiving access.

Each third-party contractor that enters into a contract or other written agreement with an educational agency under which the third-party contractor will receive student data or teacher or principal data shall:

- limit internal access to education records to those individuals that are determined to have legitimate educational interests
- not use the education records for any other purposes than those explicitly authorized in its contract;
- except for authorized representatives of the third party contractor to the extent they are carrying out the contract, not disclose any PII to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the party provides a notice of the disclosure to NYSED, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
- maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody; and
- use encryption technology to protect data while in motion or in its custody from unauthorized disclosure.

7. What steps can and must be taken in the event of a breach of confidentiality or security?

Upon receipt of a complaint or other information indicating that a third-party contractor may have improperly disclosed student data, or teacher or principal APPR data, NYSED's Chief Privacy Officer is authorized to investigate, visit, examine and inspect the third-party contractor's facilities

and records and obtain documentation from, or require the testimony of, any party relating to the alleged improper disclosure of student data or teacher or principal APPR data.
Where there is a breach and unauthorized release of PII by a by a third party contractor or its assignees (e.g., a subcontractor): (i) the third party contractor must notify the educational agency of the breach in the most expedient way possible and without unreasonable delay; (ii) the educational agency must notify the parent in the most expedient way possible and without unreasonable delay; and (iii) the third party contractor may be subject to certain penalties including, but not limited to, a monetary fine; mandatory training regarding federal and state law governing the confidentiality of student data, or teacher or principal APPR data; and preclusion from accessing any student data, or teacher or principal APPR data, from an educational agency for a fixed period up to five years.

8. Data Security and Privacy Standards

Upon appointment, NYSED's Chief Privacy Officer will be required to develop, with input from experts, standards for educational agency data security and privacy policies. The Commissioner will then promulgate regulations implementing these data security and privacy standards.

9. No Private Right of Action

Please note that Education Law §2-d explicitly states that it does not create a private right of action against NYSED or any other educational agency, such as a school, school district or BOCES.

APPENDIX S-1
Attachment to Parents' Bill of Rights
For Contracts Involving Disclosure of Certain Personally Identifiable Information

Education Law §2-d, added by Ch. 56 of the Laws of 2014, requires that a Parents' Bill of Rights be attached to every contract with a third-party contractor (as defined in the law) which involves the disclosure of personally identifiable information (PII) derived from student education records ("Student Data"), or certain teacher/principal information regarding annual professional performance evaluations that is confidential pursuant to Education Law §30212-c ("APPR Data"). Each such Contract must include this completed Attachment to provide specific information about the use of such data by the Contractor.

1. Specify whether this Contract involves disclosure to the Contractor of Student Data, APPR Data, or both.

■ Disclosure of Student Data

⬚ Disclosure of APPR Data

2. Describe the exclusive purposes for which the Student Data or APPR Data will be used in the performance of this contract.

Student Data may be utilized for the purposes of evaluating district needs, progress over time, and achievement of goals.

3. Identify any subcontractors or other persons/entities with whom the Contractor will share the Student Data or APPR in the performance of this Contract and describe how the Contractor will ensure that such persons/entities will abide by the data protection and security requirements of the Contract.

Subcontractors or other entities with whom the Contractor will share data:

The Hudson Valley RBERN will host all student data on and within our G Suite for Education interface provided by Google.

In the event the Contractor engages a Subcontractor or otherwise shares Student Data or APPR Data with any other entity, Contractor acknowledges and agrees that before any such data is shared with a Contractor or another entity, such party must agree in writing to be bound by the confidentiality and data protection provisions set forth in this Contract including, but not limited to, the "Data Security and Privacy Plan" set forth in Appendix R. Upon termination of the agreement between the Contractor and a Subcontractor or other entity, Contractor acknowledges and agrees that it is responsible for ensuring that all Student Data or APPR Data shared by the Contractor must be returned to Contractor or otherwise destroyed as provided in Paragraph 4 of the "Data Security and Privacy Plan" set forth in Appendix R.

4. Specify the expiration date of the Contract and explain what will happen to the Student Data or APPR Data in the Contractor's possession, or the possession of any person/entity described in response to Paragraph 3, upon the expiration or earlier termination of the Contract.

Contract expiration date: **June 30, 2025**

⬚ Contractor agrees to return the Student Data or APPR Data to NYSED consistent with the protocols set forth in Paragraph 4 of the "Data Security and Privacy Plan" set forth in Appendix R.

■ Contractor agrees to securely destroy the Student Data or APPR Data consistent with the protocols set forth in Paragraph 4 of the "Data Security and Privacy Plan" set forth in Appendix R.

5. State whether the Contractor will be collecting any data from or pertaining to students derived from the student's education record or pertaining to teachers or principals' annual professional performance evaluation pursuant to the Contract, and explain if and how a parent, student, eligible student (student eighteen years or older), teacher or principal may challenge the accuracy of the Student Data or APPR data that is collected.

■ Student Data

⬚ APPR Data

Any challenges to the accuracy of any of the Student Data or APPR Data shared pursuant to this Contract should be addressed to the school, educational agency or entity which produced, generated or otherwise created such data.

6. Describe where the Student Data or APPR Data will be stored (in a manner that does not jeopardize data security), and the security protections taken to ensure that the data will be protected, including whether such data will be encrypted.

Bidder should detail in this section where data will be stored, what security measures will be in place, and whether electronic data is encrypted in motion and/or at rest.

The HV RBERN fully intends to comply with Education Law §2-d. To meet the PII protection requirements of Education Law §2-d, the HV RBERN has entered into an agreement with the LHRIC, SW BOCES, Erie 1 BOCES, and Google LLC that confirms conformity to Education Law §2-d. Any potential PII hosted on and within the HV RBERN G Suite for Education interface provided by Google LLC will be covered by this agreement. Access the HV RBERN G Suite for Education is exclusively reserved to HV RBERN staff. To further provide protection for PII, access to the administrative G Suite for Education interface requires a multiple-step authentication process. This authentication process requires an initial regularly-updated password and then an additional passcode sent by SMS only to the HV RBERN Technology Specialist and/or HV RBERN Executive and Assistant Directors. It is only after these steps have been completed that administrative access to the G Suite for Education is granted.

The G Suite for Education core services are Gmail (including Inbox by Gmail), Calendar, Classroom, Jamboard, Contacts, Drive, Docs, Forms, Groups, Sheets, Sites, Slides, Talk/Hangouts and Vault. In order to protect this student data, Google encrypts Gmail (including attachments) and Drive data. All messages and data are encrypted while in motion between the HV RBERN and Google's servers as while as while at rest and in motion between Google data centers. Furthermore, Google and the G Suite do not claim ownership of any PII stored on Google servers thus ensuring the HVRBERN and NYSED retain ownership and control of PII data. The G Suite for Education core services comply with the Family Educational Rights and Privacy Act (FERPA).

This **AGREEMENT** is made and entered into as of the date of the last signature below by and between Google LLC ("Vendor"), a corporation having its principal offices at 1600 Amphitheatre Parkway, Mountain View, CA, 94043, and Erie 1 Board of Cooperative Educational Services ("Erie 1 BOCES"), a municipal corporation organized and existing under the Education Law of the State of New York having its principal offices at 355 Harlem Road, West Seneca, NY 14224. This Agreement will become effective upon the execution hereof by Vendor and Erie 1 BOCES. This Agreement will expire June 30, 2020. At that time parties may enter into a new Agreement upon terms to be agreed upon. Purchases made during the period of the Agreement will receive all products and services described in this Agreement.

WHEREAS, Google LLC has been identified and accepted by the Erie 1 BOCES as a provider of G Suite for Education, the application as more fully described in Exhibit A attached hereto and by this reference made part hereof of this Agreement (hereinafter referred to as "Product"); and

WHEREAS, a Board of Cooperative Educational Services ("BOCES") is a municipal corporation organized and existing under the Education Law of the State of New York that pursuant to Education Law §1950 provides shared computer services and software to school district components ("District" or "Districts") of the Regional Information Center ("RIC") and in that capacity purchases various products for use by said districts as part of the BOCES service, and

WHEREAS, Erie 1 BOCES is responsible for negotiating and entering into technology contracts and that other BOCES may bind themselves to such contracts and utilize services under such contracts by adopting appropriate School Board resolutions and by ordering services from Vendor by executing a Vendor "Customer Affiliate Agreement"; and

WHEREAS, this Agreement is subject to the New York's Education Law Section 2-d ("Education Law 2-d"); and

WHEREAS, several BOCES throughout New York State wish to offer G Suite for Education to its Districts as part of the BOCES service;

NOW, THEREFORE, And in consideration of the mutual promises hereinafter set forth, the parties agree as follows:

DEFINITIONS:

"**Customer Affiliate Agreement**" is the ordering document that allows Customer Affiliates to order Google Services.

"**Cooperative Service Agreement**" (COSER) is an agreement approved by the New York State Department of Education pursuant to Education Law §1950 whereby licensed Districts purchase services from a BOCES.

"**District**" means a school district component of a RIC or BOCES that purchases the Instructional Technology service COSER 7710.

"**Documentation**" means, with respect to any particular application or equipment, any applicable standard end user specifications and/or operating instructions provided by Vendor for such application and/or equipment, which may be amended from time to time. Documentation does not include any sales or marketing materials.

"**Effective Date**" means the date upon which the last Party signs this Agreement.

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

"**Licensee**" means Erie 1 BOCES on behalf of the Western New York Regional Information Center, or any other BOCES in the State of New York which accepts the provisions of this Agreement by formal action of its Board of Education.

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

"**Party**" means either Vendor or ERIE 1 BOCES.

"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.

"Personal, Private, and Sensitive Information" ("PPSI") is any information to which unauthorized access, disclosure, modification, destruction, or disruption of access or use could severely impact critical functions, employees, customers or third parties, or students in general. Private information could include one or more of the following: Social Security number; driver's license number or non-driver ID; account number, credit card number, or debit card number and security code; or access code/password that permits access to an individual's financial account or protected student records.

"**Product**" shall include each and every component specified in **Exhibit A**, which Vendor has developed, owns or which Vendor has acquired the right to license.

"Regional Information Centers" or "BOCES" mean any of the following Regional Information Centers: South Central (BT BOCES), Mohawk, Greater Southern Tier, Central New York (OCM BOCES), Northeastern (Capital Region BOCES), Monroe #1, Wayne-Finger Lakes (EduTech), Nassau, Western New York (Erie 1 BOCES), Eastern Suffolk, and Lower Hudson. It is understood that these RIC/BOCES have defined service areas within the State of New York and that said service areas include one or more "BOCES" and in that capacity purchases various software for use by said districts as part of the BOCES service. Each BOCES is an entity comprised of school districts in the state of New York. Only school districts served by a BOCES may participate in this Agreement after their BOCES Board of Education has approved the resolution and a Customer Affiliate Agreement is executed with Vendor. Licenses hosted by an individual BOCES will not be eligible for this Agreement unless and until they join the participating RIC/BOCES for this Services.

"**Services**" means any services provided by Vendor to the Licensee pursuant to any schedule, including, without limitation, consulting, educational, hosting, system administration, training or maintenance and support services.

"Student" means any person attending or seeking to enroll in a District that purchases Google products pursuant to the Agreement.

"**Shared Data**" means collectively Student Data, Teacher/Principal Data and PPSI.

"Student Data" means personally identifiable information from student records that Vendor receives from a BOCES, RIC or District.

"Teacher/Principal Data" means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of section three thousand twelve-c of New York Education Law.

"VENDOR" means Google, LLC.

1.1 Product shall be utilized at the sites as shall be designated by BOCES or District, or utilized in a cloud environment and shall be used solely for the benefit of BOCES or such District. BOCES or a District shall not permit or provide for transfer or reproduction of Product, or any portion thereof, to be placed on a computer not at the sites, by physical or electronic means, unless specifically authorized. BOCES, or a District, shall not make or allow others to make copies or reproductions of the Product, or any portion thereof in any form without the prior written consent of Vendor. The unauthorized distribution or disclosure of the Product, is prohibited, and shall be considered a material breach of this Agreement.

1.2 Except as expressly stated herein, BOCES, or a District, may not alter, modify, or adapt the Product, including

but not limited to translating, reverse engineering, decompiling, disassembling, or creating derivative works, and may not take any other steps intended to produce a source language state of the Product or any part thereof, without Vendor's prior express written consent.

1.3 BOCES, or a District, will be the sole owner and custodian of data transmitted, received, or manipulated by the Product, except as otherwise set forth in this Agreement. In the event that Vendor stores or maintains Shared Data provided to it by a BOCES, RIC or District, whether as a cloud provider or otherwise, the Vendor assumes all risks and obligations in the event of a breach of security ,of such Shared Data unless BOCES, the District, or any student causes the breach.

1.4 Vendor shall not subcontract or assign its obligation to store or maintain Shared Data provided to it pursuant to this Agreement to a third party cloud provider unless granted specific prior written permission from Erie 1 BOCES. Shared Data transferred to Vendor by a BOCES, RIC or a District will be stored in electronic format on systems maintained by Vendor in a secure data center facility located within the United States of America in accordance with the instructions received from either a BOCES, RIC or a District. The measures that Vendor will take to protect the privacy and security of the Shared Data while it is stored in that manner are those associated with industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

1.5 Subject to the terms of the Vendor`s Data Processing Amendment (incorporated by reference into this Agreement under Exhibit A) and unless otherwise prohibited by statute or court order, Vendor must promptly inform the BOCES, RIC or District, as applicable, in the event that any Shared Data it stores or maintains pursuant to this Agreement, including such data as may be stored or maintained by a third party cloud provider on Vendor's behalf, is requested by law enforcement authorities or otherwise sought by subpoena or court order.

1.6 Vendor will keep confidential all information and data, including any Shared Data, to which it has access in the performance of this Agreement.

1.7 In addition to the above requirements, for Shared Data as defined above:

A. Vendor shall maintain the confidentiality of the Shared Data in accordance with applicable state and federal law. Vendor acknowledges that the New York State Education Department is in process of promulgating regulations to ensure compliance with Education Law 2-d and that upon its adoption of those Education Law 2-d regulations, it may become necessary for the parties to adopt an amendment that supersedes or supplements the terms of this Agreement. Vendor agrees to act in good faith to take such additional steps to adopt all necessary documents so the terms of the Agreement will be in compliance with Education Law 2-d and its implementing regulations.

B. Vendor's data security and privacy plan for how all state, federal and local data security and privacy contract requirements will be implemented over the term of this Agreement, consistent with Erie 1 BOCES' policy on data security and privacy, is described in the G Suite for Education terms of service and the G Suite Data Processing Amendment.

C. Vendor's data security and privacy plan includes Erie 1 BOCES' Parents Bill of Rights for data privacy and security (a copy of which is attached hereto and incorporated into this Agreement as Exhibit B.

D. In accordance with Vendor's data security and privacy plan, Vendor agrees that any of its officers or employees, and any officers or employees of any subcontractor or assignee of Vendor, who will have access to the Shared Data, have received or will receive training on the federal and state law governing confidentiality of such data prior to receiving the data or access to the data. Upon request, Vendor and/or its subcontractors or assignees will provide a certification from an appropriate officer that the requirements of this paragraph have been satisfied in full.

E. The exclusive purposes for which Vendor is being provided access to the Shared Data is: to provide Licensees

with the functionality of Google G Suite for Education Services.

F. Vendor will ensure that it will only share Shared Data with additional third parties if those third parties are contractually bound to observe the same obligations to maintain data privacy and security as required by Vendor pursuant to this Agreement.

G. Upon expiration of this Agreement without renewal, Vendor shall, if requested in advance by BOCES, RIC or a District, assist BOCES, RIC or the District in exporting all electronically stored Shared Data previously received back to the BOCES, RIC or a District for a period that shall not exceed 180 days after the Agreement's termination or expiration date ("Transition Term"). The G Suite for Education Terms of Service (including payment obligations) will continue to apply during the Transition Term. Thereafter, Vendor shall promptly securely delete and/or dispose of any and all Shared Data remaining in the possession of Vendor or its assignees or subcontractors (including all electronic versions or electronic imaging of hard copies of Shared Data) in accordance with the terms of G Suite Data Processing Amendment. Vendor agrees that neither it nor its subcontractors or assignees will retain any copy, summary or extract of the Shared Data or any related work papers on any storage medium whatsoever. At the end of the Transition Term, Vendor will have no further obligation to provide the terminated Services and will cease providing such Services without any further notice.

H. In the event that a Parent or Eligible Student wishes to challenge the accuracy of the Shared Data concerning that Student or Eligible Student that is maintained by Vendor, that challenge may be processed through the procedures provided by the licensed District for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Vendor's services allow the District to promptly correct any inaccurate data stored in Vendor's systems. A teacher or principal who wishes to challenge the accuracy of the Shared Data concerning that teacher or principal that is maintained by Vendor may do so through the process set forth in the APPR plan of their employing school district or BOCES.

I. Shared Data received by Vendor or by any subcontractor or assignee of Vendor from a BOCES, RIC or a District shall not be sold or released for any commercial purposes, nor shall it be sold or used for marketing purposes.

J. Vendor acknowledges that it has the following additional obligations under NYS Education Law 2-d with respect to any Shared Data received from a BOCES, RIC or a District, and agrees that any failure to fulfill one or more of these statutory obligations shall be deemed a breach of this Agreement, as well as subject Vendor to various penalties under Education Law 2-d, including but not limited to civil penalties:

   a. To limit internal access to education records and Student Data to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA); e.g., the individual needs access to the Student Data in order to fulfill his or her responsibilities in performing the services provided to a BOCES, RIC or a District by Vendor;

   b. To not use education records or Shared Data for any purpose(s) other than those explicitly authorized in this Agreement;

   c. To not disclose any Personally Identifiable Information to any other party who is not an authorized representative of Vendor using the information to carry out Vendor's obligations under this Agreement, unless:
      i. the Parent or Eligible Student has provided prior written consent, or
      ii. the disclosure is required by statute or court order, and notice of the disclosure is provided to the BOCES, RIC or District prior to the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

K. To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of PII in its custody;

L. To use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2), or any other technology or methodology specifically authorized by applicable statute, regulation or the NYS Education Department;

M. To notify the BOCES, RIC or a District of any breach of security resulting in an unauthorized release of Shared Data by Vendor or its subcontractors or assignees in violation of applicable state or federal law, the Parents Bill of Rights for student data privacy and security, the data privacy and security policy of Erie 1 BOCES, and obligations relating to data privacy and security within this Agreement including the Vendor's Data Processing Amendment in the most expedient way possible and without unreasonable delay. Notifications related to any data incident or breach of data will be subject to the terms of the Vendor's Data Processing Amendment.

N. In the event that a BOCES, RIC or a District is required under Education Law 2-d to notify Parent(s) or Eligible Student(s) of an unauthorized release of Shared Data by Vendor or its assignees or subcontractors, Vendor shall promptly reimburse the BOCES, RIC or a District for the full cost of such notification.

O. BOCES, or a District, shall keep confidential the Product and all Documentation associated therewith whether or not protected by copyright. BOCES, or a District, will reasonably protect such information and at a minimum provide the same safeguards afforded its own like confidential information. Confidential information shall not include information in the public domain, information already rightfully in the possession of the other party without an obligation to keep it confidential, information obtained from another source without obligations of confidentiality, information independently developed, or information required by a court or government order or applicable law.

P. Vendor shall have the right upon, three business days written notice to BOCES or District, as applicable, to enter the premises of the BOCES or the District for the purpose of inspecting to ensure compliance by the BOCES or the District of its obligations hereunder. Entry shall only be allowed Monday through Friday during the normal business hours or 8:00 A.M. to 3:00 P.M. Eastern Time.

1.8 To the extent that any term of the G Suite for Education terms of service directly conflicts with the terms of this Agreement, the terms of this Agreement shall apply and be given effect.

Vendor agrees that the terms of this Agreement may be shared with any BOCES or District or representatives thereof.

Any District may bind itself and Vendor to the terms of this Agreement by opting into the terms of this Agreement in writing by executing a Customer Affiliate Agreement. Vendor's recourse in the event of a breach of this Agreement by any District or BOCES shall be limited to recourse against the breaching District or BOCES and shall not extend to any other District or BOCES.

ADDITIONAL TERMS

As to Section 1.4, the Erie 1 BOCES acknowledges and agrees that Vendor and its affiliates use a range of subprocessors to assist with the provision of the G Suite Service. More information about Vendor's subprocessor use can be found at this link: https://gsuite.google.com/intl/en/terms/subprocessors.html.

Notwithstanding anything to the contrary under Section 1.4, in reference to the storage location for data, for certain Vendor G Suite editions, BOCES and/or a District may select data regions for the storage of data. Data regions allow administrators to store covered data in a specific geographic location (the United States or Europe) by using a data region policy. BOCES and/or District are individually responsible for assessing whether Vendor data regions feature complies to applicable requirements. Vendor data regions policy can be found at this link: https://support.google.com/a/answer/7370133?hl=en complies with Licensee applicable laws.

Vendor protects Shared Data, and our agreements address how we do that. Before Vendor discloses confidential information in accordance with a legal process, Vendor will use commercially reasonable efforts to promptly notify you of that disclosure, unless otherwise prohibited by statute or court order. More information about Vendor privacy can be found in the G Suite terms of service.

Licensee may sign a Vendor Data Processing Amendment, which exclusively describes the processing and security of customer data under the applicable customer agreement.

As to data security and privacy training and notwithstanding anything to the contrary in Section 1.7.D, Vendor clarifies that it has training and policies that apply to Vendor employees and vendors. In addition to mandatory training, Vendor privacy policies include Google's Privacy Policy, Google Privacy and Security Principles, Internal Privacy Policies, Information Security Policies, and the Google Code of Conduct. Data privacy and security related to Google subprocessors can be found in the Data Processing Amendment referenced above.

Licensee has the ability to export customer data from Vendor's systems at any time according to the terms of the Data Processing Amendment.

Customer: ERIE 1 BOCES	**Vendor: Google LLC**
By:	By: Philipp Schindler 2019.09.30 08:59:30 -07'00'
Print Name: James Fregelette	Print N Philipp Schindler Authorized Signatory
Title: Executive Director, Admin & Operations	Title:
Date: 9/26/19	Date:

EXHIBIT B

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

(1) A student's Personally Identifiable Information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record.

(3) State and federal laws protect the confidentiality of Personally Identifiable Information, 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.

(4) A complete list of all Student Data elements collected by the State is available for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of Student Data addressed.

Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be directed to the Chief Privacy Officer via email at: CPO@mail.nysed.gov.

Google LLC ("Vendor")

Signature Philipp Schindler
Authorized Signatory

Title

Date 2019.09.30 08:59:48 -07'00'

APPENDIX

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services, Erie 1 BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law.

Each contract the BOCES enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include the following information:

(1) the exclusive purposes for which the student data or teacher or principal data will be used;

(2) how the third-party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

(3) when the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

(4) if and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

(5) where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

EDUCATION LAW 2-d OPT-IN

This Education Law 2-d Opt-In ("Opt-In") is executed and entered into as of the date of execution specified below ("Effective Date"), by the School District identified below ("District").

WHEREAS, Google LLC ("Vendor"), a corporation having its principal offices at 1600 Amphitheatre Parkway, Mountain View, CA, 94043, provides certain services to the District pursuant to certain contractual arrangements and Vendor Terms of Service ("TOS") entered into between District and Vendor; and,

WHEREAS, the State of New York has enacted New York Education Law 2-d; and,

WHEREAS, Erie 1 Board of Cooperative Educational Services ("Erie 1 BOCES"), a municipal corporation organized and existing under the Education Law of the State of New York having its principal offices at 355 Harlem Road, West Seneca, NY 14224, has entered into an EDUCTION LAW 2-d Agreement ("Agreement") in order to address and give binding effect to the terms of New York Education Law 2-d and Section 1.8 of which Agreement provides that school districts can become party to the Agreement by executing a written opt-in to do so; and,

WHEREAS, District wishes to become party to the Agreement;

NOW THEREFORE, District attests and agrees as follows:

1. District has evaluated its needs with respect to New York Education Law 2-d and wishes to become subject to the terms of the Agreement;

2. District hereby formally notifies Erie 1 BOCES and confirms that it is opting into the Agreement in accordance with Section 1.8 thereof.

3. By executing this Opt-In, District agrees to be bound by and to comply with the terms of the Agreement.

EXECUTED:

DISTRICT: Hudson Valley Regional Bilingual Education Resource Network (RBERN)

EXECUTED BY: _____

NAME: Stephen Tibbetts

TITLE: Asst Supt for Bus & Admin Services

DATE: 1/13/20