SCHEDULE E

EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Noiz Ivy, Inc. d/b/a OYOClass.com (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Board of Cooperative Educational Services, First Supervisory District of Suffolk County ("ESBOCES") and Contractor, including any Agreement to Terms attached thereto, to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that ESBOCES' and/or participating school districts' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"**Protected Data**" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by ESBOCES and/or participating school districts. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of ESBOCES and/or participating school districts as that term is defined in § 99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of ESBOCES and/or participating school districts relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with ESBOCES' policy(ies) on data security and privacy. Contractor shall promptly reimburse ESBOCES and/or participating school districts for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of ESBOCES' and/or participating school districts' data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of ESBOCES' and/or participating school districts' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;

3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

6. Specifies whether Protected Data will be returned to ESBOCES and/or participating school districts, transitioned to a successor contractor, at ESBOCES' and/or participating school districts' option and direction, deleted or destroyed by the Contractor when the contract and/or the Agreement to Terms is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);

2. Comply with the data security and privacy policy of ESBOCES; Education Law § 2-d; and Part 121;

3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

    a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

    b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;

7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and

8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of ESBOCES' or participating school district's Parents' Bill of Rights.

NOIZ IVY, INC. D/B/A OYOCLASS.COM

BY: ______________________ **DATED:** 5.12.21

Data Security and Privacy Plan

New York State Education Law 2-d was enacted in 2014 to address concerns relative to seeming certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, **Noiz Ivy Inc. d/b/a OYOCLASS** hereby establishes the following data security and privacy plan:

Noiz Ivy Inc. d/b/a OYOCLASS will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as it uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. **Noiz Ivy, Inc. d/b/a OYOCLASS** shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. **Noiz Ivy, Inc. d/b/a OYOCLASS** shall not use Protected Data for any other purposes than those explicitly provided for in its agreement with the disclosing party from which it received Protected Data. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Noiz Ivy Inc. d/b/a OYOCLASS shall have in place sufficient internal controls to ensure that Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, CIPA, FERPA and HIPAA, if applicable.

"Protected Data" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by a customer. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

"Personally identifiable information" from student records of an educational Vendor as that term is defined in §99.3 of the Family Educational Rights and Privacy Act (FERPA),

-AND-

Personally identifiable information from the records of an educational Vendor relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law 3012-c.

State, federal, and local data security and privacy contract requirements will be implemented by utilizing Best practices and industry standards with respect to data storage, privacy and protection, including, but not limited to encryption, firewalls, passwords, protection of off-site records, and limitations of access to stored data to authorized staff shall be implemented as follows:

[*DESCRIBE WHAT METHODS WILL BE USED TO PROTECT DATA*]

OYOCLASS (a/k/a OYOCLASS.com) is a web-based learning platform making available educational resources and creative development tools that allow individuals, whether teacher, student or administrator, to engage and self-lead the development of information-based resources that can be shared across a distributed network, such as the internet.

The purpose of **OYOCLASS** is to instruct principles and practices of computer science/engineering, digital literacy, entrepreneurship and other STEAM (science, technology, engineering, art, math) related outcomes for individuals to engage as they are required, or is desired personally. As a result of this operational objective, **OYOCLASS** is designed to provide maximum flexibility and control over the data that individuals using the **OYOCLASS** platform exercise personally.

Most connections to **OYOCLASS** and its associated resources are encrypted (HTTPS) by default, via continuously updated SSL certificates. As numerous domains are used in provisioning differentiated technical services within the **OYOCLASS** platform, some may not include encrypted connections based on the type of activity being engaged and technical feasibility of doing so.

Noiz Ivy Inc. d/b/a OYOCLASS respects DNT ("Do Not Track") settings in browsers. While logged out of our Services, and having DNT enabled in browser, we may still use cookies for analytics and measurement purposes, but we will not load any third-party trackers (e.g. Google Analytics). By logging in, individuals are opting to allow **Noiz Ivy Inc. d/b/a OYOCLASS** to ignore the DNT setting and to use 3rd party data tools to provide a personalized experience. Our use of 3rd party data tools is limited to services such as Google Analytics, for the purposes of improving our services only, and delivering to clients the experience they desire.

All sessions that individuals inaugurate within **OYOCLASS** platform by creating an account (defining a sign-in ID, password, email address) will only be used/useful contextually, within the class deployment or community that an account is registered to access. **Noiz Ivy Inc. d/b/a OYOCLASS** provides a unique method to account holders to maintain their personal identification contextually, by permitting the creation of "Alias" identifiers within **OYOCLASS** implementations, so that the individual is in control of how they represent themselves when navigating between school and community organizations, such as libraries, Universities and other community education partners using the **OYOCLASS** platform.

All sign-in ID related password data is encrypted and stored in a secure manner on **OYOCLASS** servers. Individuals will be allowed to request their sign-in ID or password hints via email communication, in the event it is forgotten by individual. Individuals may also change their sign-in ID and password at their own discretion at any time.

OYOCLASS is designed to permit personal data possession and portability of the creative resources that individuals design and develop within **OYOCLASS**, or with **OYOCLASS** tools. All accounts maintain the ability to take the creative outputs of their efforts and their personally possessed data with them by downloading such data at any time.

Given the complexity of providing a service that enables the creation of data in numerous computer programming languages and computing paradigms, the methods enabled to provide individuals with the option of possessing their creative data will evolve over time, and in every case will attempt to increase the control that individuals have over their personal data.

As the creative data that is created within **OYOCLASS** may take the form of both open source and private resources under the control and definition of individual accounts, **OYOCLASS** cannot make a statement on how such data will be used within and without the **OYOCLASS** platform. This choice is dependent on individual account owners, and the manner they use to create and share their data-based outcomes. However, to the greatest degree possible, using methods designed by **OYOCLASS**, all personally identifiable information (PII) that an account binds to their creative work, shall remain under the control of the individual account holder, and in the case where schools wish to control how data is organized and used by students, this PII data shall take the form that is decided upon by school officials. Once shared, data that is open may not be secured as exclusively private. Prior to sharing, all data accessed at **OYOCLASS** and created within **OYOCLASS** is only accessible by those account holders with contextual permission to join the learning community being supported by **OYOCLASS** where data is accessed.

OYOCLASS was created with the idea that "owning your own" data is fundamental to the creative learning process that **OYOCLASS** enables. **Noiz Ivy Inc. d/b/a OYOCLASS** will never use or cause to be used by any other entity outside of our direct client contracted relationships, the data that belongs to individual account owners and school districts, in an inappropriate manner. **Noiz Ivy Inc. d/b/a OYOCLASS** may from time to time share creative data contributed by account owners openly, with sharing permitted in the design of such data, for the purposes of promoting student work, classroom work, school district work, teacher work, or the, web-based systems enabling such creativity. Some of the tools enabled by **OYOCLASS** empower teachers, administrators and students to also share openly the creative work being implemented within **OYOCLASS**, and may from time to time provide insight into the activity happening within otherwise closed and private learning spaces.

To the greatest degree possible, **Noiz Ivy Inc. d/b/a OYOCLASS** limits the types of data that are collected from our clients in beginning a relationship and setting up accounts for students, teachers and administrators.

The disclosure of PII data is of utmost concern to **Noiz Ivy Inc. d/b/a OYOCLASS**, and in the course of developing learning outcomes, will be openly discussed with students, teachers and administrators within **OYOCLASS** learning tools and curriculum to increase the vigilance and dexterity with which such data is interacted with by all people. In the event failures happen, **Noiz Ivy Inc. d/b/a OYOCLASS** will work to rectify the matter, no matter who causes the failure, or how the failure was created. This goal is directly related to the mission that **Noiz Ivy Inc. d/b/a OYOCLASS** services as an education provider.

Measures to secure Protected Data and to limit access to such data to authorized staff will include:

All **Noiz Ivy Inc. d/b/a OYOCLASS** representatives, employees, contractors will be required to sign a non disclosure and confidentiality Agreement prior to working with client data. An educational process will include training internal staff on the appropriate methods of accessing secured data, interacting with secured data, and participating in secure learning communities where data is being created and used by clients.

Noiz Ivy Inc. d/b/a OYOCLASS performs background checks on all internal personnel interacting with secured data.

We're committed to ensuring the security of our infrastructure and our users' data.
Each of the facilities we co-locate with enforces multiple layers of security via a variety of technological and human measures. Beyond that, all our equipment is in locked cages.
We enforce strict filtering rules to ensure that all server nodes can only communicate using their allowed IP addresses.
This prevents nodes from spoofing other nodes' IPs or performing man-in the-middle attacks on our private network.

Our server resources themselves operate within KVM or Xen virtualization, which ensures that each node has its own kernel and userspace, which are fully separate from other nodes. This ensures that a malicious node cannot access either the host itself or other nodes' resources.

All **Noiz Ivy Inc. d/b/a OYOCLASS** files and data are backed up every 24 hours to prevent loss of data to the greatest degree possible, as caused by equipment failure, natural disasters or nefarious outcomes.

Noiz Ivy Inc. d/b/a OYOCLASS provides our clients with access control methods which may be custom deployed by clients, and provide different internal staff with different levels of access to the information resources within **OYOCLASS**. These same access controls are used by **Noiz Ivy Inc. d/b/a OYOCLASS** with our own internal staff relationships to provision appropriate access to data resources as needed.

Subcontractors, persons or entities with which **Noiz Ivy Inc. d/b/a OYOCLASS**will share Protected Data, if any, will abide by the requirements of this data security and privacy plan, and any contractual obligations with respect to Protected Data set forth in the agreement with the disclosing party.

Internal access to Protected Data shall be limited to those individuals that are determined to have legitimate educational interests.

Protected Data shall not be used for any other purposes than those explicitly authorized by contract with an educational Vendor.

Protected Data shall not be re-disclosed to any third-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 the New York State Education Department, educational Vendor, 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;

Reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of Protected Data shall be maintained.

Encryption technology shall be used to protect data while in motion or in **Noiz Ivy Inc. d/b/a OYOCLASS'** custody from unauthorized disclosure.

EASTERN SUFFOLK BOCES
PARENTS' BILL OF RIGHTS
FOR DATA SECURITY AND PRIVACY

Eastern Suffolk BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information. The Agency wishes to inform the school community of the following rights:

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 maintained by Eastern Suffolk BOCES.

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.

Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Claudy Damus-Makelele
Associate Superintendent for Educational Services
Eastern Suffolk BOCES
201 Sunrise Highway
Patchogue, NY 11772
cdamus@esboces.org

Or in writing to:

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, New York 12234.
CPO@mail.nysed.gov

Supplemental Information Regarding Third-Party Contractors:

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk 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." Each contract the Agency enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include information addressing the following:

1. The exclusive purposes for which the student data or teacher or principal data will be used;

Provisioning an account, with access controls, and allowing student/teacher to access services.

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;

   No data will be shared that exposes personally identifiable information, subcontractors (mentors) will only see anonymous data when interacting with student/teacher information. All subcontractors will receive training, and be held accountable to best practices when interacting with student/teacher data.

3. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

   Data remains accessible directly to student/teacher, while access to community resources will expire, and student/teachers will be archived from community use of resources. All personally created data will remain intact, for permanent access control by creators.

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

   Complaints should be directed to: the Associate Superintendent for Curriculum for your district; Or in writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234, CPO@mail.nysed.gov.

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.

   All data will be stored securely in the United States, according to data security plan, and encrypted during transport for access by students/teachers.

Third Party Contractors are required to:

1. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
2. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
3. Not use educational records for any other purpose than those explicitly authorized in the contract;
4. Not disclose personally identifiable information 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 third-party contractor provides a notice of the disclosure to the New York State Education Department, 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;
5. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
6. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;
7. Notify Eastern Suffolk BOCES of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;
8. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
9. Provide a signed copy of this Bill of Rights to Eastern Suffolk BOCES thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

A copy of this ESBOCES Parents' Bill of Rights must be made a part of Contractor's Data Security and Privacy

Plan.