Supplemental Information for Agreement with _Noiz Ivy Inc dba OYOclass.com (hereinafter "Third-party Contractor"): For purposes of further ensuring confidentiality and security of student data, each contract ("Agreement") the Mineola Union Free School District (the "District") enters into with a third-party contractor (the "Third-party Contractor") shall include a Data Security and Privacy Plan that includes a signed copy of the District's Parents' Bill of Rights and in which Plan the Third-party Contractor agrees to abide by the District's Parents' Bill of Rights and to comply with the following:

1) **Exclusive Purposes for which Student Data Will Be Used.** Use of Personally Identifiable Information ("PII") under the Agreement will be limited to that necessary for the Third-party Contractor to perform the duties outlined in the Agreement and the services associated with that function. The Third-party Contractor further agrees that no PII will be sold or used for marketing or commercial purposes.

2) **Protective Measures Regarding Third Parties.** The Third-party Contractor will ensure that any subcontractor or other person or entity with whom the Contractor shares student data and/or teacher or principal data, if applicable, agrees to abide by all of the components of applicable state and federal law, including New York Education Law Section 2-d, the District's Parents' Bill of Rights, and the Family Educational Rights and Privacy Act ("FERPA"). In addition, the Third-party Contractor will ensure that each subcontractor, person or entity with whom the Third-party Contractor shares student data and/or teacher or principal data will abide by all the terms and conditions of this Data Security and Privacy Plan.

3) **Expiration of Agreement.** Absent renewal, the Agreement expires annually on June 30th. If the District does not renew the Agreement past June 30th of the contractual year, all student data shall be deleted, within 90 days, in accordance with the National Institute of Standards and Technology (NIST) standard 800-88. The Third-party Contractor will ensure, at the sole discretion of the District, that all student data are returned to the District or provide confirmation to the District that the data in its possession has been securely destroyed. The Third-party Contractor will also ensure that all emails containing personally identifiable student information are returned to the District and deleted from the Third-party Contractor's email account. Third-party Contractor shall ensure that any data it retains after 90 days is data it is required to retain by law and retention is secured in accordance with NIST and/or HIPPA standards.

4) **Challenge to Accuracy of Data.** A parent, student, teacher or principal can challenge the accuracy of the Data received or generated by the Third-party Contractor in writing addressed to Whittney Smith, Ed.D., Director of Instructional Technology and Assessment, Mineola Union Free School District, 2400 Jericho Turnpike, Garden City Park, New York 11040.

5) **Storage of Data.** Student data shall be stored in a secure data center using monitoring of the access doors, fire and security monitoring, system health and intrusion monitoring, data backups and retentions. Data storage and access shall comply with the Advanced Encryption Standard (AES) with minimum of 128 bit key encryption or better.

6) **Breach of Personally Identifiable Information.** The Third-party Contractor must notify the District of any breach or unauthorized release of PII within seven (7) calendar days of any such breach or Third-party Contractor's knowledge of such breach. The Third-party Contractor shall promptly reimburse the District and/or its Participants for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of PII by the Third-party Contractor, its subcontractors, and/or assignees.

MINEOLA UNION FREE SCHOOL DISTRICT	THIRD-PARTY CONTRACTOR
By: Cheryl Lampasona	By:
Name: Cheryl Lampasona	Name: Melora Loffreto
Title: President, Board of Education	Title: Executive Director

OYOCLASS

Data Security and Privacy Plan

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, OYOCLASS hereby establishes the following data security and privacy plan:

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. 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. 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, 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 agency 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 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 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 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.

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 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 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. 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 can not 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 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. 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. 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, 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 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, 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 OYOCLASS services as an education provider.

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

[DESCRIBE WHAT METHODS WILL BE USED TO PROTECT DATA]

All 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.

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 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.

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 OYOCLASS with our own internal staff relationships to provision appropriate access to data resources as needed.

Subcontractors, persons or entities with which 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 agency.

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 agency, 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 OYOCLASS's custody from unauthorized disclosure.