

GARDEN CITY UNION FREE SCHOOL DISTRICT
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 _____ (the "Contractor") is a covered third-party contractor.

Noiz Ivy Inc dba OYOclass.com

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the GARDEN CITY UNION FREE SCHOOL DISTRICT (the "District") and Contractor 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 the District's 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 the District. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

"Personally identifiable information" from student records of the District as that term is defined in § 99.3 of FERPA,

-AND-

"Personally identifiable information" from the records of the District 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 District policy(ies) on data security and privacy. Contractor shall promptly reimburse the District 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 the District's 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 the District's 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 the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the contract 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 the District; 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.

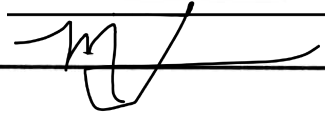
In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

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 the District's Parent Bill of Rights.

NAME OF PROVIDER: Noiz Ivy Inc dba OYOclass.com, Melora Loffreto

BY: _____



DATED: _____

7/23/25

Return to:

Lauren Maguire
Director of Information Technology
Garden City Union Free School District
56 Cathedral Avenue
Garden City, NY 11530
maguirel@gcufsd.net

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

OYOclass Privacy Policy

We built OYOclass so people like you could create or join learning and teaching communities. To make this happen, we collect some information for our users. The OYOclass Team understands how important privacy is to our communities, especially kids and parents. We wrote this privacy policy to explain what information we collect, how we use it, and what we're doing to keep it safe. If you have any questions regarding this privacy policy, you can contact us.

Please DO NOT share personal identifiable information (PII), such as your physical address, email address, phone number, or anything else that can be used to make contact outside of the OYOclass platform. Please report projects, comments, or discussion posts that contain this kind of information so the OYOclass team can remove it, and please remind the author of our policy to protect the privacy of all account owners.

What information does OYOclass collect about me?

Account Information: In order to create or join a community, you need to make an account. During account creation, we ask you to define a sign-in name, an accurate email address (or your parent or guardian's email address if you are under 13 years old), and a password for securely accessing your account. There is no requirement that you use a sign-in name that correlates to your legal name or other format that could be used to identify you generally, and we suggest that you use a sign-in name known only to you, and that you keep this information private and secure personally also. Your sign-in name will only be used by you to sign-in to the OYOclass platform and access our services, and will not be used to publicly identify you within the platform.

If you subscribe to a mailing list of a community which is built with OYOclass, your email for subscription can be viewed by the creator (owner) of that community, as this information is necessary for the community owner to keep you updated on requested information. If you are a community owner, you are responsible for protecting and using

subscriber emails to provide requested information resources, and not spamming them with abusive content.

User-generated Content:

For all OYOclass account owners, you will be provided with a profile and portfolio that you may customize for your own purposes, and these shall contain an optional avatar portrait, your display alias, skill listings, project work, biography information and custom information you choose to store on the OYOclass servers as a representation of your learning activities, which can be viewed by others based on your setting of view permissions. At all times, you will maintain control and responsibility for the accurate representation of your own personally defined and shared information, and may alter this information, and its visibility at any time personally. All personal data representing your learning and publishing activities shall persist within OYOclass servers until such time as you choose to download and/or delete such data personally. As an OYOclass account owner, the portability and right to delete personal information remains under your personal control at all times;

Parents may request access to student accounts at any time, for inspection of learning and publishing activities. As of the latest update to this privacy policy, and in recognition of the laws of the States we conduct business within, OYOclass.com Agrees to provide remedies for parents to enforce the protection of student data in all cases where need is present and identified. OYOclass.com learning platform is proactive in addressing the privacy protection of students, and to the greatest degree possible provides mechanisms of direct control, as well as instructional guidance to increase the digital literacy of all our platform users. It is the mission of our organization to increase digital literacy and personal data control in all of our interactions with young people, and work with parents to ensure the use of the tools in OYOclass platform are engaged as intended, and for the empowerment of students. Parents in New York should also reference the "Parents Bill of Rights for Data Privacy and Security", Education Law §2-d here: [Parents Bill of Rights](#).

For community creators, all of your community data, including your community name, events, blogs, pages, email campaigns, courses, challenges, micro-credentials, discussion posts are also stored on the OYOclass servers. Other users can view your published blogs, events, forum posts, courses, along with your community name based on permissions that you define within your private community.

For community members, your joined communities, membership, joined events, discussion posts are stored on the OYOclass servers, and can be viewed by others within these communities.

The OYOclass Team is responsible for moderation of community activities, and maintains access to all content stored on the OYOclass servers, including unpublished content, so that we may assist community owners and members from time to time as requested, or contractually obligated.

Usage Information: When you use OYOclass, our servers will automatically store a limited amount of information about how you use the website. This information includes a number that identifies your computer (the IP address), which pages you visited, and what browser you are using.

Analytics: In order to optimize our services, we also collect some data on where you click and which parts of the site you visit. This “click data” helps us figure out ways to improve the website. Information collected and processed includes the user’s IP address, network location, geographic location, web browser information and device information.

Cookies: When you visit the OYOclass website or OYOclass generated community website, it asks your browser to put an http "cookie" on your computer. The cookie is actually a small text file that our site can send to your browser for storage on your computer. This allows the website to remember that you are logged in when you go to a different page.

How does OYOclass use my information?

We will use your email address to respond to messages you send us or to communicate with you about OYOclass service or your account. Your email will allow you to administer password reminders and sign-in name reminders when you require assistance.

If we detect repeated abusive behavior from your account or IP address, we may share your account name, IP address, and the time and content of the abusive behavior with the IP address owner (such as a school or internet service provider).

We may use de-identified location, age, gender, and usage data in our own internal research studies intended to improve our understanding of how people learn with OYOclass, for the purpose of improving our tools.

We may disclose some information we collect to third-party service providers that help us manage communications to and from OYOclass website and improve website performance strictly in support of app functionality. No personal usage data is shared with 3rd parties. We remain vigilant to ensure that these service providers have privacy policies that restrict them from further disclosing any of the information disclosed in providing their services. No personally identifiable information shall be disclosed in these activities.

How can I update my personal information?

You can update your password, email address, and alias information through the Account Settings page. You can also reset your password through the Password Reset page. Additionally, all of your personal learning activities and any project-based data can be updated on your profile and portfolio pages, as well as in the editors wherein this data is created and managed personally.

How does OYOclass protect my information?

OYOclass has in place physical and electronic procedures to protect the information we collect on OYOclass website. We strictly limit individual access to the OYOclass servers and the data we store on them. However, as effective as these measures are, no security system is impenetrable. We cannot completely guarantee the security of our database, nor can we guarantee that the information you supply will not be intercepted while being transmitted to us over the Internet. We utilize https encryption methods to protect data in transit, respect DNT browser settings to provide users control of how they are tracked through the use of cookies, and backup all data to provide redundant security and integrity for all account owners personal data.

Notifications of Changes to the Privacy Policy

We review our security measures and Privacy Policy on a periodic basis, and we may modify our policies as appropriate. We may also change or update our Privacy Policy if we add new services or features. If we make any changes to our privacy practices, we will amend this Privacy Policy accordingly and post the amended policy on OYOclass website. We encourage you to review our Privacy Policy on a regular basis.

Last change: 5.21.2025