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 Everest Web Deals LLC (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 Huntington 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 and/or Participants' 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"), 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 and/or a Participant. 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 and/or its Participants as that term is defined in § 99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of the District and/or its Participants 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 and/or its Participants 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 and/or its Participants' data, 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 and/or its Participant's Protected Data, shall maintain a Data Security and Privacy Plan that aligns with the NIST Cybersecurity Framework and includes the following elements:

1. A provision incorporating the requirements of the District's Parents' Bill of Rights for data security and privacy, to the extent that any of the provisions in the Bill of Rights applies to Contractor's possession and use of Protected Data pursuant to this Agreement.

2. An outline of how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the Contractor's policy on data security and privacy.

3. An outline of the measures taken by Contractor to secure Protected Data and to limit access to such data to authorized staff.

4. An outline of how Contractor will use "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.

5. An outline of how Contractor will ensure that any subcontractors, persons or entities with which Contractor will share Protected Data, if any, will abide by the requirements of Contractor's policy on data security and privacy, and the contractual obligations with respect to Protected Data set forth herein.

Contractor shall ensure any the subcontractors, persons or entities that Contractor will share Protected Data with, if any, will abide by contractual obligations with respect to Protected Data set forth herein.

Contractor hereby acknowledges that it is aware of and agrees to abide by the District's Bill of Rights, attached. A copy of this signed document must be made a part of Contractor's data security and privacy plan.

SIGNATURE: _____

TITLE: CEO

DATE: 10/14/2026

DATA PRIVACY AND SECURITY PLAN

1. Appendix A, Contractor's Data Privacy and Security Plan, is included.
2. A copy of the District's Bill of Rights is included with this document.

APPENDIX A — DATA PRIVACY AND SECURITY PLAN

Choice Eliminator for Google Forms

Prepared October 14, 2026 from Everest Web Deals' published product, privacy, and security disclosures. Items requiring company confirmation are listed in Section 6.

1. Purpose and scope

Choice Eliminator manages choice limits, option availability, schedules, notifications, and response-management functions in Google Forms. It uses the installer-authorized Google account and product configuration to provide those features.

2. Data categories and handling

Data category	Collection, use, and storage
Installer and license	Installer name and email are used for Google authentication, license activation, account support, and service communications. Everest retains account and licensing records.
Form configuration	The product profile identifies form structures, choice configurations, custom URLs, and payment transaction references as stored product records. The privacy policy says form configurations are encrypted on secure U.S. servers; the Security & Privacy Center identifies AWS U.S. infrastructure.
Submitted responses	Google Forms submissions remain in the customer's Google account. Everest's product privacy policy says response answers are not saved or stored on Everest servers. Response counts, Response Manager edits, and reset workflows may be processed in real time through the authorized Google account to provide the selected feature.
Payments	Stripe or PayPal handles license checkout and payment-card data directly. The product supports optional Stripe payment workflows; the Security & Privacy Center lists Stripe transaction references among stored Choice Eliminator records. Exact fields and retention for form-payment transactions require confirmation.
Support	Support email conversations and the email address are retained for reference. Information voluntarily provided for troubleshooting may also be retained as needed.

AI use: Choice Eliminator does not use AI. No form content or response data is sent to an AI provider for Choice Eliminator features.

3. Storage, access, and service providers

The original form and respondent submissions remain in Google Workspace under the customer's account. Everest stores installer and licensing information plus product configuration needed to operate the add-on. Published disclosures state that configurations are encrypted and hosted on U.S. servers. Google services provide the form and authentication platform; AWS is listed for encrypted hosting and configuration storage. Stripe or PayPal may process payments. AI providers are not used for this product.

The Security & Privacy Center states that support staff do not review form or student content. The product privacy policy states that Everest does not access the installer's Gmail mailbox.

4. Retention, deletion, and correction

Configuration records are retained as needed to provide the configured feature. Account and license records are retained while active and for a reasonable support, security, billing, or audit period. Support communications are retained to resolve customer issues and related needs. The published policy permits deletion requests through everestwebdeals@gmail.com. Form owners manage response records in Google Forms; Response Manager can edit or delete records through the authorized account. The public disclosures do not specify a per-field retention schedule or a secure return process at the end of a district contract.

5. Security controls stated in the published disclosures

The product privacy policy states that form configurations are encrypted on secure U.S. servers and that Everest uses technical and organizational measures to protect personal information. The Security & Privacy Center identifies AWS infrastructure in the United States. The published product materials do not describe NIST Cybersecurity Framework alignment, encryption-in-transit details, key management, firewall/network controls, access-log review, backup controls, or staff training procedures.

6. Items requiring company confirmation

1. Confirm whether Everest accepts this rider, including the NIST-alignment requirement, District policies, staff-training duties, encryption requirements, and subcontractor flow-down terms.
2. Confirm the technical controls and access restrictions that will apply to District information, including encryption in transit and at rest, authorized staff access, and any training records.
3. Confirm District-specific breach notice timing and contacts, reimbursement of notification costs, and the process for return or deletion at contract expiration.
4. Confirm retention details for configuration, account, support, and optional Stripe transaction-reference records, including any District-specific deletion request.

7. Public sources reviewed

Choice Eliminator product page: https://everestwebdeals.co/en/form-choice-eliminator/

Choice Eliminator privacy policy: https://everestwebdeals.co/en/policy-form-choice-eliminator/

Security & Privacy Center: https://everestwebdeals.co/en/security-privacy-center/

Accessed October 14, 2026.

HUNTINGTON UNION FREE SCHOOL DISTRICT

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Pursuant to New York State 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, as defined by Education Law §2-d. This document contains a plain English summary of such 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 educational records maintained by the Huntington Union Free School District.

3. State and Federal Laws protect the confidentiality of personally identifiable student 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 New York State is available for review at the following website:

   http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx

   The list may also be made available by writing to:

   Office of Information & Reporting Services
   New York State Education Department
   Room 863 EBA,
   89 Washington Avenue
   Albany, NY 12234

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

   Huntington Union Free School District
   Attn: Beth Mccoy, Superintendent
   50 Tower Street
   Huntington Station, New York 11743
   Email: Bmccoy@hufsd.edu
   Phone: 516-673-2038

   OR

   Chief Privacy Officer

New York State Education Department
89 Washington Avenue
Albany, NY 12234

Email: CPO@mail.nysed.gov

6. Each contract with a third-party contractor which will receive student data, or teacher or principal data will include information addressing the following:

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

   d. If and how a parent, student, a student over eighteen years of age, 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, and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

7. Third-party contractors are also required to:

   a. 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;

   b. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.

   c. Not use educational records for any other purpose than those explicitly authorized in the contract;

   d. 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;

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

f. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;

g. Notify the Huntington Union Free School District 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;

h. 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;

i. Provide a signed copy of this Bill of Rights to the Huntington Union Free School thereby acknowledging that they aware of and agree to abide by this Bill of Rights.

8. 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.

Third-Party Acknowledgement

As a third-party contractor, I acknowledge that our contract with the Huntington Union Free District necessitates the receipt of student data and as such, requires adherence with NY State Education Law 2-d and the District's Parents' Data Bill of Rights for Data Privacy and Security. In this regard, we acknowledge our responsibility to adhere to the noted elements of the document, and have instituted processes to abide by same.

Name Nazokat Position CEO
Company: Everest Web Deals LLC

Signature _____ Date 10/14/2026