ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

1050 Main Street
Roseville, CA 95678
Phone (916) 771-1645

Data Privacy Agreement

This Agreement is entered into between the **Roseville City School District** ("LEA" or "District") and

Ner Chat Inc.
"Service Provider" or "Vendor"

("Service Provider" or "Vendor") on

08/31/2026
Effective Date

WHEREAS, the LEA and the Service Provider entered into an agreement for educational or digital services to the LEA;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed, or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms; and

WHEREAS, the provider and LEA agree that additional and modified sections are required to address the use of Artificial Intelligence ("AI") as part of the services or product provided;

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. PASSWORD SECURITY: All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator, or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

Vendor Attestation:

Agree

2. SYSTEM SECURITY: Unauthorized access to or modification of District systems, including file servers, routers, switches, NDS, and Internet services, is prohibited. Any attempt to bypass or subvert any District security system, both hardware and software, is prohibited.

Vendor Attestation:

Agree

3. PRIVACY: The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code, and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties protected and confidential. Release of this data can be authorized only by Technology Services management and by state and federal law.

Vendor Attestation:

Agree

4. REUSE: Vendors shall not copy, duplicate, sell, repackage, or use for demonstration purposes any Roseville City School District data without the prior written consent of Educational or Technology Services management.

Vendor Attestation:

Agree

5. TRANSPORT: The Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.

Vendor Attestation:

Agree

6. EXTERNAL SECURITY: The Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.

Vendor Attestation:

Agree

7. INTERNAL SECURITY: Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personnel (or their representatives) will have directly with District data. How is the data uploaded from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protect against unauthorized access to District data? How are backups performed, and who has access to and custody of the backup media? How long are backups maintained? What happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard-copy records?

Vendor Attestation:

Agree

8. DISTRICT ACCESS: The Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).

Vendor Attestation:

Agree

9. TERMINATION: Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. The Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.

Vendor Attestation:

Agree

Section II: AB1584 Compliance - Student Information Only

1. The Vendor agrees that the Roseville City School District retains ownership and control of all student data.

Vendor Attestation:

Agree

2. The Vendor must attach a description of how student-created content can be exported and/or transferred to a personal account to this document.

Vendor Attestation:

Not Applicable

Export Student-Created Content Not Applicable

Students create nothing — no accounts.

3. The Vendor is prohibited from allowing third parties access to student information beyond those purposes defined in the contract.

Vendor Attestation:

Agree

4. The Vendor must attach a description of how parents, legal guardians, and students can review and correct their personally identifiable information to this document.

Vendor Attestation:

Agree

5. The Vendor will attach to this document evidence of how student data is kept secure and confidential.

Vendor Attestation:

Agree

6. The Vendor will attach to this document a description of the procedures for notifying affected parents, legal guardians, or eligible students when student records are unauthorizedly disclosed.

Vendor Attestation:

Agree

7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled.

Vendor Attestation:

Agree

8. The Vendor will attach to this document a description of how they and any third-party affiliates comply with FERPA.

Vendor Attestation:

Agree

9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students.

Vendor Attestation:

Agree

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.

Vendor Attestation:

Agree

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.

Vendor Attestation:

Agree

3. Vendors cannot sell student information.

Vendor Attestation:

Agree

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety, or operational improvement reasons.

Vendor Attestation:

Agree

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

Vendor Attestation:

Agree

6. Vendors must delete district-controlled student information when requested by the District.

Vendor Attestation:

Agree

7. Vendors must disclose student information when required by law, for legitimate research purposes, and for school purposes to educational agencies.

Vendor Attestation:

Agree

Section IV: Audit and Compliance Oversight

1. Audit Rights. The District reserves the right to audit the Vendor's privacy and security practices no more than once annually or at any time in response to a data incident, suspected noncompliance, or legal/regulatory inquiry. The Vendor shall provide reasonable access to systems, records, and personnel involved in the handling of District data.

2. Confidentiality Agreement. RCSD agrees to execute a reasonable non-disclosure agreement to protect Vendor trade secrets or proprietary information disclosed during the audit.

3. Framework Compliance. Vendor agrees to implement and maintain security controls consistent with one or more of the following frameworks:

a. NIST Cybersecurity Framework (NIST CSF)

b. NIST SP 800-53 or 800-171

c. ISO/IEC 27001

d. CIS Critical Security Controls (Top 18)

The Vendor shall indicate which framework is used and provide a summary upon request.

Designated Security Framework(s):

NIST Cybersecurity Framework (CSF), NIST SP 800-53, and CIS Critical Security Controls.

4. Security Program Documentation. Upon request, the Vendor shall furnish RCSD with the following:

a. A summary of its data security policies and incident response procedures.

b. Results from the most recent third-party security assessment or audit, redacted as necessary.

c. Any certifications (e.g., SOC 2, ISO 27001).

5. Remediation Obligations. If a security deficiency or compliance failure is identified, the Vendor shall deliver a written remediation plan to RCSD within thirty (30) days. The District may suspend access to its data until the deficiency is addressed to the District's satisfaction.

6. Subprocessor Oversight. The Vendor is responsible for ensuring that all subprocessors or affiliates with access to District data comply with the terms of this agreement and are subject to equivalent audit and compliance obligations.

Exhibits

Section 1.6: External Security

Glint is hosted in AWS us-east-1 within an isolated VPC. AWS Security Groups and Network ACLs provide stateful firewalling, and public access is HTTPS-only over port 443 enforcing TLS 1.2 or higher. The MongoDB Atlas database is VPC-peered with no public endpoint and is unreachable from the internet. AWS GuardDuty provides continuous intrusion detection with CloudWatch alarming and escalation under our documented incident response plan. Vulnerability management includes quarterly dynamic application security testing via HCL AppScan, continuous static analysis via SonarCloud, and continuous dependency scanning via Dependabot. Firewall configuration is reviewed annually; the most recent review was completed November 2024 and is available on request.

Section 1.7: Internal Security

Ner Chat personnel have no routine interaction with District data. The District does not transmit data files to Ner Chat, and Ner Chat does not connect to or extract from District systems — there is no roster sync and no student information system integration. District staff create their own accounts or authenticate via District-managed SSO, and create their own content. Access to production is governed by role-based access control under least privilege, with multi-factor authentication required for engineering, administrative, and billing roles and access reviews conducted quarterly. Safeguards include AES-256 encryption at rest, TLS 1.2+ in transit, and audit logging of logins, resource activity, administrative actions, and security-relevant changes, retained a minimum of 30 days with user ID, IP address, and timestamp. Backups are automated through AWS and MongoDB Atlas, encrypted at rest, stored separately from production, and accessible only to authorized engineering personnel with MFA; there is no physical or removable backup media, and restore testing is performed annually. Ner Chat produces no printed records of District data.

Section II.2: Exporting of Student-Created Content

Not applicable. Glint is a teacher-facing platform. Students do not have accounts, do not log in, and do not create content within the application. All content is created by educators and clinical staff, so there is no student-created content to export or transfer to a personal account. Staff users may export the visual supports they create, and those materials remain under District control.

Section II.4: Review and Correct Personally Identifiable Information (PII)

Glint does not collect or store student data and holds no student personally identifiable information to review or correct. Requests are directed to the District, which remains the point of contact for families and retains ownership and control of all District data. Ner Chat responds to a District-forwarded request for access within 45 days, or within the period required by applicable law, whichever is sooner, and corrects any identified factual inaccuracy within 90 calendar days of District notice. Staff users may review, correct, and delete their own account information and created content directly within the application at any time. Requests may be sent to Scott Soifer, CTO, at scott@nerchat.com.

Section II.5: Securing Student Data

Glint does not collect or store student data, so no student record exists within the platform to be exposed or disclosed. The platform holds only staff account credentials (name and work email), application metadata such as IP address and cookie data, usage statistics, and the visual supports staff create. It does not hold student names, identifiers, dates of birth, addresses, email addresses, photographs, roster, enrollment, attendance, assessment, or health records. All platform data is protected by AES-256 encryption at rest and TLS 1.2+ in transit, RBAC with least privilege, MFA on privileged roles, quarterly access reviews, VPC isolation with no public database endpoint, GuardDuty and CloudWatch monitoring, and encrypted automated backups with annual restore testing. Subprocessors are limited to AWS, MongoDB Atlas, and OpenAI, the latter under a Business Associate Agreement and Modified Abuse Monitoring agreement excluding customer content from monitoring logs and model training. No student data is disclosed to any subprocessor because none exists within the platform.

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

Glint is a teacher-facing tool and does not collect or store student data. The platform holds no student education records, so FERPA protections attaching to education records have no records within Glint to which they apply. Ner Chat nonetheless commits that the District retains ownership and control of all District data; that all District data is treated as confidential and released only as authorized by the District or required by law; that District data is never copied, sold, repackaged, or used for demonstration purposes without prior written consent; that no District information is used to target advertising and no student profile is created for any purpose; and that subprocessors are contractually bound to equivalent confidentiality obligations and receive no student data. Should the platform's scope ever change such that student data would be collected, Ner Chat will notify the District immediately and will not implement the change without District review.

Section III.5: How Student Data is Protected:

Glint does not collect or store student data, so no student record exists within the platform to be exposed, misused, or disclosed. The platform holds only staff account credentials (name and work email), application metadata such as IP address and cookie data, usage statistics, and the visual supports created by educators and clinical staff. It does not hold student names, identifiers, dates of birth, addresses, email addresses, photographs, roster, enrollment, attendance, assessment, conduct, or health records. All platform data is protected by AES-256 encryption at rest and TLS 1.2+ in transit, role-based access control under least privilege, multi-factor authentication on privileged roles, quarterly access reviews, VPC isolation with no public database endpoint, AWS GuardDuty and CloudWatch monitoring, and encrypted automated backups with annual restore testing. Ner Chat maintains a formal incident response plan with defined severity levels, escalation paths, and breach notification procedures, and notifies the District within 72 hours of confirming any incident affecting District data. Subprocessors are limited to AWS, MongoDB Atlas, and OpenAI, the latter under a Business Associate Agreement and Modified Abuse Monitoring agreement that excludes customer content from monitoring logs and model training. Ner Chat implements security controls consistent with the NIST Cybersecurity Framework, NIST SP 800-53, and the CIS Critical Security Controls.

Required Security & Compliance Attachments

Please upload all required documentation referenced in this agreement, including evidence of external and internal security controls, data protection practices, compliance certifications (e.g., SOC 2, ISO 27001), incident response procedures, and any required FERPA, SOPIPA, or AB 1584 compliance documentation.

Attachments should clearly correspond to the sections outlined in the Data Privacy Agreement.

Upload

[Private File Not Included]

ARTIFICIAL INTELLIGENCE (AI) ADDENDUM

Section A: Applicability Declaration

Please select the appropriate response below:

○ **Option 1: Applicable (AI Deployment Active)** ◉ **Option 2: Not Applicable (No AI Deployment)**

Option 1: Applicable (AI Deployment Active)

The Service Provider currently uses, embeds, or leverages AI features, models, or third-party AI sub-processors to deliver Services to the District.

- **Required:** Provider must comply with all sections of this Addendum.
- **Action:** Review all requirements and execute the signature block below.

Option 2: Not Applicable (No AI Deployment)

The Service Provider does not currently use, embed, or leverage AI features or third-party AI services in connection with District Student Data or Services.

- **Waived:** Sections 1 and 3–10 do not apply.
- **Required:** Provider must comply with Section 2.1 (Future Deployment Notification).
- **Action:** Sign the signature block below to execute this waiver.

Section B: AI Governance Terms

1. AI Usage Limitations, Ownership & Third-Party Models

1.1. The Service Provider shall not use, transfer, or reproduce Student Data for Artificial Intelligence (AI) training, model development, fine-tuning, or content generation without the District's prior written consent. The Provider agrees to uphold the principles outlined in California Education Code §33328.5, ensuring that any AI systems used in connection with the Service align with values of equity, safety, transparency, and accountability in the interest of student welfare.

1.2. Sub-licensing Student Data for such purposes is strictly prohibited unless explicit written permission is obtained from the student's parent, legal guardian, or eligible student.

1.3. Ownership of all Student Data, including content generated with AI assistance, remains with the District or the student, as applicable.

2. Notification and Consent

2.1. If any feature of the Service is modified to include AI functionality (or if a non-AI provider intends to introduce AI features), the Provider shall notify the District in writing prior to deployment.

2.2. The Provider must disclose the specific AI architecture (including third-party tools used), the purpose of such use, and how Student Data will be processed within these features.

2.3. No AI feature may be enabled until the District provides written consent and has reviewed any updated data-handling practices.

3. Algorithm Bias and Fairness

3.1. The Provider certifies that any AI technologies used in facilitating the Services (whether proprietary or integrated via third parties) are regularly audited for algorithmic bias and fairness.

3.2. Upon request by the District, the Provider shall furnish a summary of audit findings related to bias detection and mitigation strategies. For third-party embedded AI, providing official third-party audit reports or compliance attestations shall satisfy this requirement. These audits shall demonstrate commitment to promoting equitable outcomes and addressing systemic bias under California Education Code §33328.5(d).

4. AI Hallucinations and Reliability

4.1. The Provider shall monitor the hallucination rate of any deployed generative AI models (e.g., large language models or chatbots) and employ industry-standard techniques to reduce the occurrence of inaccurate or misleading outputs.

4.2. The Provider shall maintain a mechanism for the District to report hallucinated or harmful responses and address such issues in a timely and accountable manner

5. Prohibited Uses of AI

The Provider shall not (and shall ensure its sub-processors do not):

5.1. Use AI to generate synthetic or inferred Student Data.

5.2. Develop behavioral profiles for marketing or advertising.

5.3. Engage in predictive analytics that may result in automated decision-making affecting students without human oversight.

5.4. Deploy AI systems that are not designed to minimize harmful outcomes to minors, including but not limited to biased academic profiling or discriminatory content outputs.

These prohibitions align with California Education Code §33328.5(c), which calls for educational AI technologies to be designed to minimize harm and safeguard the well-being of students.

6. Student Content and AI-Generated Work

If students create content using AI tools embedded in the Service (e.g., essays, responses, or projects), the Provider shall:

6.1. Ensure students can download or export that content.

6.2. Retain no ownership or claim over AI-assisted student work.

6.3. Maintain logs of AI interactions in accordance with FERPA.

6.4. Support digital literacy and public awareness regarding the use of AI, in accordance with §33328.5(b), by enabling users to understand when they are interacting with an AI system.

7. Transparency and Disclosure Requirements (SB 942)

7.1. To the extent required by California SB 942, the Provider shall maintain and make available tools or mechanisms to verify whether content was generated by AI, including provenance data where applicable. This tool shall:

7.1.1. Provide provenance data (excluding personal data).

7.1.2. Support multiple content formats.

7.1.3. Accept user feedback to support continuous improvement.

7.2. All AI-generated content must include latent disclosures that identify:

7.2.1. The Provider's name.

7.2.2. Identification of the AI system used.

7.2.3. The creation date and time.

7.2.4. A unique identifier for the generated content.

7.3. The Provider shall also offer users the option to include visible disclosures indicating that the content was generated by AI. These disclosures must be conspicuous and designed to resist removal.

7.4. If the Provider licenses its AI technology to third parties, such license agreements shall require those third parties to uphold the same transparency and disclosure standards outlined herein.

8. Third-Party AI Sub-processors & Embedded Tools

8.1. Flow-Down Obligations: If the Provider embeds, integrates, or queries third-party AI models or APIs (e.g., OpenAI, Anthropic, Azure OpenAI), the Provider remains fully responsible for ensuring such third parties comply with the privacy, non-training, and security standards set forth in this Addendum.

8.2. Zero-Data Retention / No Training Guarantee: The Provider certifies that all third-party AI integrations operate under enterprise API agreements that strictly prohibit the third-party AI vendor from retaining, logging, or using Student Data to train their underlying models.

8.3. Exemptions for Standard Third-Party Infrastructure: Where the Provider leverages external foundation models, compliance with Sections 3 (Auditing) and 7 (Provenance) may be fulfilled by providing the underlying vendor's published safety, transparency, and audit documentation.

9. Definitions

9.1. Artificial Intelligence (AI): Systems that analyze data and take actions, with some degree of autonomy, to achieve specific goals.

9.2. Hallucination: A response generated by an AI system that is incorrect, nonsensical, or misleading while appearing factually accurate.

9.3. Algorithmic Bias: Systematic and unfair discrimination in outcomes generated by an algorithm based on characteristics such as race, gender, or disability.

10. Compliance with State Advisory Guidelines

10.1. The Provider shall monitor and cooperate with any guidance or recommendations issued by the California Department of Education's Artificial Intelligence in Education Advisory Council, as established under Education Code §33328.5(a). This cooperation may include participation in feedback initiatives, alignment with recommended practices, or revisions to data governance protocols in response to evolving regulatory requirements.

Service Provider Signature	Date Signed
ScottSoifer	08/31/2026 01:05 pm

DATA INCIDENT NOTIFICATION ADDENDUM

This Exhibit outlines the Vendor's obligations in the event of a Data Incident involving Customer Data. These obligations are in addition to and do not limit any rights or remedies available to the Customer under the Agreement or applicable law.

1. Data Incident Notification

1.1. In the event Roseville City School District ("RCSD" or "District" or "Customer") Data is accessed, acquired, or reasonably believed to have been accessed or acquired by an unauthorized individual or third party ("Data Incident"), the Vendor shall notify the Customer in writing without undue delay, and in no case later than seventy-two (72) hours after confirming the occurrence of the Data Incident.

1.2. The Vendor shall comply with all reasonable instructions from the District in relation to the Data Incident and, in consultation with the District, take all appropriate and reasonable steps to investigate and mitigate any known or anticipated harmful effects resulting from such unauthorized access, use, or disclosure of Customer Data.

1.3. If the Data Incident involves Personally Identifiable Data (PII), including but not limited to Social Security numbers, government-issued identification numbers, financial account details, health records, or medical information protected under applicable privacy laws (e.g., HIPAA, FERPA, CCPA, SOPIPA, GDPR, CRPA, etc), the Vendor shall apply heightened protections in accordance with applicable state and federal law, including but not limited to breach notification, identity theft prevention, and mitigation requirements.

2. Notification to Affected Individuals and Authorities

The obligations in this Section apply in all cases where the Data Incident is caused, in whole or in part, by the actions or omissions of the Vendor, its subcontractors, or affiliates.

2.1. Following confirmation of a Data Incident, the vendor shall provide written notification to affected individuals whose data was compromised. This notification shall:

2.1.1. Be written in plain language;

2.1.2. Be delivered in compliance with applicable federal, state, or provincial laws;

2.1.3. Be issued without unreasonable delay following the District's approval and any required consultation with law enforcement

2.2. The notification to affected individuals shall include, at a minimum:

2.2.1. A general description of the incident and the Vendor's response efforts.

2.2.2. The contact information of the Vendor's designated incident response representative.

2.2.3. The type(s) of Customer Data or PII involved (e.g., name, address, date of birth, Social Security number, student records, health/medical information, etc.);

2.2.4. The known or estimated date(s) of the Data Incident and the date of notification.

2.2.5. Whether law enforcement was involved and whether any delay in notification was due to a law enforcement investigation.

2.2.6. Steps the individual can take to protect themselves.

2.3. The Vendor agrees to adhere to all applicable federal, state, and provincial laws concerning the protection of Customer Data, including but not limited to the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and the Health Insurance Portability and Accountability Act (HIPAA), where applicable.

In the event of a Data Incident involving Personally Identifiable Information (PII) of a minor, the Vendor acknowledges that PII includes both direct and indirect identifiers that could reasonably identify an individual student. Under FERPA, PII includes, but is not limited to:

• Student's full name

• Student identification number or state/local student identifier

• Date and/or place of birth

• Grade level or classroom assignment

• School name or teacher name

• Mailing address or contact information

• Parent/guardian names and contact information

• Any combination of the above elements that would reasonably allow identification of the student with reasonable certainty

2.4. If such PII is involved in a Data Incident, the Vendor shall:

2.4.1. The Vendor shall fully fund and coordinate identity monitoring and/or credit monitoring services for a minimum of twelve (12) months, including, at a minimum, dark web monitoring, identity theft insurance, and access to fraud resolution agents, without cost to the affected individual or the District.

2.4.2. As described in Section 2.2, notify all affected individuals (or their legal guardians, as applicable).

2.4.3. If five hundred (500) or more individuals are affected, the Vendor shall notify the appropriate State Attorney General or supervisory authority in accordance with relevant state data breach laws and ensure that the notification complies with all timing, format, and content requirements set forth under the relevant state's breach notification statute. A copy of the regulatory notification shall be provided to the Customer.

2.4.4. Maintain a record of the Data Incident, including the nature of the breach, categories of data affected, notification steps taken, and services provided. Upon request, the customer will have access to these records.

2.4.5. The Vendor shall ensure that all breach response and notification processes are consistent with applicable FERPA guidance and any other relevant federal, state, or provincial privacy regulations. No PII shall be re-disclosed or shared with any third party, including subcontractors or affiliated entities, without prior written consent from the District or as explicitly required by law. The Vendor shall document and maintain detailed records of all data disclosures related to the incident and shall make those records available to the District upon request.

3. Legal Compliance and Risk Management

The Vendor agrees to comply with all applicable local, state, provincial, and federal data privacy and security laws, including but not limited to:

- Family Educational Rights and Privacy Act (FERPA)
- Children's Online Privacy Protection Act (COPPA)
- Health Insurance Portability and Accountability Act (HIPAA)

State-specific data breach notification statutes

3.1. The Vendor shall maintain a written incident response and breach notification policy that complies with industry standards and applicable law. The Vendor shall, upon request, make a summary of its policy available to the District.

3.1.1. The Vendor shall ensure that any subcontractor, service provider, or third party with access to Customer Data is contractually bound by equivalent or stronger data protection, confidentiality, and incident response obligations as outlined in this Agreement. The Vendor shall remain fully responsible for any acts or omissions of such third parties in connection with the handling of Customer Data.

3.2. At the District's request, and where such assistance is not unduly burdensome, the Vendor shall provide reasonable cooperation and support for any investigation, regulatory inquiry, or litigation arising out of or relating to the Data Incident, including support in notifying affected individuals and interfacing with regulatory authorities.

3.3. The Vendor shall not disclose the existence or details of a Data Incident to any third party, including media, regulators, or other customers, without the District's prior written approval, except as strictly required by law.

3.4. In no event shall the District be held financially liable for any costs, damages, regulatory penalties, or legal expenses arising from a breach of Customer Data caused, in whole or in part, by the Vendor, its subcontractors, or affiliates. The Vendor shall be solely responsible for all costs associated with investigation, response, notification, remediation, credit or identity monitoring, and any regulatory or legal actions stemming from such a breach.

3.5. The Vendor shall fully indemnify, defend, and hold harmless the District from and against any and all claims, damages, liabilities, penalties, costs, and expenses (including reasonable attorneys' fees) arising from or related to a Data Incident caused, in whole or in part, by the Vendor, its subcontractors, or agents. This includes, but is not limited to, costs associated with breach notification, regulatory inquiries, litigation, and third-party claims.

Service Provider Signature	Date Signed
ScottSoifer	08/31/2026 01:05 pm

This Agreement constitutes the entire understanding among the Parties with respect to the subject matter hereof and supersedes all prior agreements, whether written or oral. No amendment or modification of this Agreement shall be valid unless in writing and signed by authorized representatives of both Parties.

As an authorized representative of my organization, I accept the conditions listed in this document.

Authorized Representative Signature

Service Provider

Date

08/31/2026 01:05 pm

Service Provider

Name

Scott Soifer

Service Provider

Title

CTO

Service Provider

Email (Service Provider)

scott@nerchat.com

Service Provider

Date

08/31/2026 10:39 am

Roseville City School District

Name

Laura Assem

Roseville City School District

Title

Executive Director, Technology Services

Roseville City School District

Ner Chat, Inc. (“Glint”)

Security & Privacy Addendum

Roseville City School District — Data Privacy Agreement

Required Security & Compliance Attachment

Field	Detail
Provider	Ner Chat, Inc. (product: Glint)
Prepared by	Scott Soifer, Chief Technology Officer
Address	5 Tideway St, Kings Point, NY 11024
Contact	scott@nerchat.com · 516-404-3479
Date	August 28, 2026
Purpose	Supporting documentation for attestation items in Sections I, II, and III

Statement of Platform Scope

Glint is a teacher-facing tool. It does not collect or store student data.

Glint is used by educators, therapists, and clinical staff to generate visual supports — communication boards, schedules, and social stories. Only staff hold accounts and log in. Students are not users of the platform, do not have accounts, and have no information stored about them. A completed board may be shared with a student or family via a link or QR code, but the student does not interact with the system and nothing about the student is captured.

Glint is not a student information system, not a learning management system, and is not roster-synced. No District student data is transmitted to, processed by, or stored within the platform.

The following sections correspond to the numbered attestation items in the District’s Data Privacy Agreement.

Index of contents

Section III.5 — How Student Data is Protected	Securing Student Data
Section IV — Framework and certifications	Appendix

Section I.6 — External Security

The District requests evidence that the system is secure from external attack, with firewalls and NAT as a minimum and active IDS or equivalent preferred. Glint meets the preferred tier.

Hosting and network perimeter

- All infrastructure is hosted in Amazon Web Services (AWS), region us-east-1 (Northern Virginia). All data is processed and stored on United States servers.
- Application resources run inside an isolated Virtual Private Cloud (VPC). AWS Security Groups and Network ACLs provide stateful firewalling at the instance and subnet level.
- Public access is HTTPS-only over port 443, enforcing TLS 1.2 or higher. No other inbound ports are exposed to the internet.
- The MongoDB Atlas database is VPC-peered to the application VPC. There is no public database endpoint and the database is not reachable from the internet.
- A firewall configuration review is performed annually. The most recent review was completed in November 2024 and is available on request.

Threat detection and monitoring (IDS-equivalent)

- AWS GuardDuty provides continuous intrusion detection and threat monitoring across accounts, workloads, and network activity.
- AWS CloudWatch provides logging, metric alarms, and alerting on security-relevant events.
- Security event alarms are configured to escalate to engineering under the documented incident response plan.

Encryption

- Data at rest is encrypted using AES-256.
- Data in transit is encrypted using TLS 1.2 or higher.

Vulnerability management

- Quarterly dynamic application security testing (DAST) using HCL AppScan.
- Continuous static application security testing (SAST) using SonarCloud on every pull request.
- Continuous third-party dependency and vulnerability scanning using Dependabot.
- Secure development lifecycle including peer code review, staging validation, environment segregation, and formal change approval before production deployment.

Disclosure: Ner Chat does not currently hold a third-party penetration test report. External security validation is performed through the quarterly DAST program described above. A third-party penetration test is planned as part of ongoing SOC 2 maturity work.

Section I.7 — Internal Security

The District's questions are answered individually below.

Describe the interactions vendor personnel (or their representatives) will have directly with District data.

Ner Chat personnel have no routine interaction with District data. The District does not transmit data files to Ner Chat, and Ner Chat does not connect to, query, or extract from District systems. District staff create their own accounts (or authenticate through District-managed single sign-on) and create their own content. Engineering personnel access production systems only for maintenance, troubleshooting, and support, under the access controls described below.

How is the data uploaded from the District handled and processed?

No bulk data upload from the District occurs. There is no roster sync, no student information system integration, and no file transfer of District records. The only information entering the platform is the staff account information required for login (name and work email address) and the instructional content that staff themselves create.

Who has access to this data?

Access is governed by role-based access control (RBAC) under a least-privilege model. Multi-factor authentication is required for all privileged access, including engineering, administrative, and billing roles. Access rights are reviewed quarterly and revoked promptly on role change or separation. Access to production systems is limited to a small number of named engineering personnel.

What happens to the data after the upload is complete?

Not applicable in the conventional sense, as no District data upload occurs. Content created by staff is stored in the encrypted production database and remains available to the authoring staff user for the life of the account.

What security safeguards are in place to protect against unauthorized access to District data?

Encryption at rest (AES-256) and in transit (TLS 1.2+); VPC network isolation with no public database endpoint; RBAC with least privilege; multi-factor authentication on privileged roles; quarterly access reviews; AWS GuardDuty threat detection; CloudWatch alarming; and audit logging of logins and logouts, resource create/read/update/delete activity, administrative actions, and security-relevant configuration changes. Log records include user ID, IP address, and timestamp and are retained for a minimum of 30 days.

How are backups performed, and who has access to and custody of the backup media?

Backups are automated and performed through AWS and MongoDB Atlas, using continuous backup together with point-in-time snapshots. Backups are encrypted at rest and stored logically separate from production. There is no physical or removable backup media; custody remains within the AWS and MongoDB Atlas environments under Ner Chat's control. Access to backups is limited to authorized engineering personnel with multi-factor authentication. Restore testing is performed annually; a full user account was successfully restored from backup within approximately two hours during an actual incident.

How long are backups maintained?

[CONFIRM — state the exact backup retention window configured in AWS and MongoDB Atlas, e.g. "continuous backup with a 7-day point-in-time recovery window and snapshots retained for 30 days."]

What happens to the District data once the backup is expired?

Expired backups are deleted automatically by the platform provider at the end of the retention window and the underlying storage is released and overwritten. No expired backup copies are retained, exported, or archived elsewhere.

If any data is printed, what happens to these hard-copy records?

Ner Chat does not print District records. No hard-copy records of District data are produced, handled, or stored by Ner Chat personnel. Visual supports printed by District staff for classroom use are created and controlled entirely by the District.

Section II.2 — Export of Student-Created Content

Marked Not Applicable.

Glint is a teacher-facing platform. Students do not have accounts, do not log in, and do not create content within the application. All content is created by educators and clinical staff. There is therefore no student-created content to export or transfer to a personal account.

Staff users may export and retain the visual supports they create, and those materials remain under District control.

Section II.4 — Review and Correction of Personally Identifiable Information

Glint does not collect or store student data, and consequently holds no student personally identifiable information that a parent, guardian, or eligible student would need to review or correct. Ner Chat nonetheless maintains the following process.

- Requests are directed to the District, which remains the point of contact for families and retains ownership and control of any District data.
- Ner Chat responds to a District-forwarded request for access to data within 45 days, or within the period required by applicable law, whichever is sooner.
- Where a factual inaccuracy is identified, Ner Chat corrects the record within 90 calendar days of notice from the District.
- Staff users may review, correct, and delete their own account information and the content they have created directly within the application at any time.
- Requests may be submitted to Scott Soifer, CTO, at scott@nerchat.com.

Sections II.5 and III.5 — Securing Student Data

These items request evidence that student information is protected through reasonable security procedures and practices.

The controlling fact is that Glint does not collect or store student data. There is no student record within the platform to be exposed, misused, or disclosed. The security program described below protects all platform data, including the staff account information and instructional content that the platform does hold.

Information the platform holds

- Staff account credentials, limited to name and work email address.
- Application technology metadata, including IP address and cookie data.
- Usage statistics reflecting staff interaction with the application.
- Visual supports created by staff, including symbol and image selections drawn from the platform library.

Information the platform expressly does not hold

- Student names, student identifiers, dates of birth, addresses, or email addresses.
- Student photographs or recordings.
- Roster, enrollment, attendance, assessment, conduct, or transcript data.
- Grade-level or class-level data tied to an identified student.
- Health, medical, or clinical records concerning students or patients.

Controls

- Encryption: AES-256 at rest, TLS 1.2+ in transit.
- Access: RBAC with least privilege, MFA on privileged roles, quarterly access reviews.
- Network: VPC isolation, no public database endpoint, HTTPS-only public access.
- Monitoring: AWS GuardDuty and CloudWatch, with audit logging retained for a minimum of 30 days.
- Testing: quarterly DAST, continuous SAST, continuous dependency scanning.
- Resilience: encrypted automated backups, documented business continuity and disaster recovery plan, annual restore testing.

Subprocessors

Ner Chat performs due diligence on all vendors and relies on SOC 2 or ISO-aligned providers. No student data is disclosed to any subprocessor, because none exists within the platform.

- Amazon Web Services — hosting and infrastructure.
- MongoDB Atlas — database services.
- OpenAI — AI content generation, under a Business Associate Agreement and a Modified Abuse Monitoring agreement. Customer content is excluded from OpenAI monitoring logs and is not used to train OpenAI models.

Glint is not a conversational interface. Staff select a topic and a template, and the system returns a structured visual board. Inputs are structured prompts, not free-form conversation, and the system does not request or collect student personal information.

Incident response and notification

Ner Chat maintains a formal incident response plan with defined severity levels, escalation paths, and breach notification procedures. In the event of a confirmed unauthorized disclosure affecting District data, Ner Chat notifies the District within 72 hours of confirmation and supports the District in any notification it elects to make to parents, guardians, or eligible students. Ner Chat does not hold parent or guardian contact information and therefore does not notify families directly.

Retention and deletion

District-controlled data is deleted on District request. On expiration or cancellation of the contract, customer data is permanently deleted within 90 days, subject only to retention required by applicable state or federal law. Certification of destruction is available on request. No student records are retained or made available to any third party following termination.

Section II.8 — FERPA Compliance

Glint is a teacher-facing tool and does not collect or store student data. The platform holds no student education records, and FERPA protections attaching to student education records therefore have no records within Glint to which they apply.

Ner Chat nonetheless operates under the following commitments.

- The District retains ownership and control of all District data at all times.
- All District data is treated as confidential. Data is released only as authorized by the District or as required by state or federal law.
- District data is never copied, duplicated, sold, repackaged, or used for demonstration purposes without prior written District consent.
- No District information is used to target advertising. Ner Chat does not operate an advertising business and does not build advertising profiles.
- No student profile is created for any purpose.
- Subprocessors are contractually bound to equivalent confidentiality and data protection obligations and receive no student data.
- Personnel with access to production systems are bound by confidentiality obligations and trained on data handling responsibilities.

Should the platform's scope ever change such that student data would be collected, Ner Chat will notify the District immediately and will not implement the change without District review.

Appendix — Framework Alignment and Certification Status

Provided in support of Section IV. Ner Chat states its position accurately rather than claiming certifications it does not hold.

Designated security frameworks

- NIST Cybersecurity Framework (CSF)
- NIST SP 800-53
- CIS Critical Security Controls

A control summary for each framework is available on request.

Certification status

Item	Status
SOC 2 Type II	In progress via Vanta. Not yet certified.
ISO/IEC 27001	Aligned with the framework. Not certified.
Third-party penetration test	Not on file. Quarterly DAST via HCL AppScan.
HIPAA	Aligned with HIPAA practices. BAA available on request.
Accessibility (WCAG 2.1 AA)	Internal conformance review. No third-party VPAT.

Prepared and attested by:

Scott Soifer
Chief Technology Officer, Ner Chat, Inc.
scott@nerchat.com · 516-404-3479