ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

STUDENT DATA PRIVACY AGREEMENT

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Peachjar, Inc. ("Service Provider" or "Vendor") on 07/18/2025 ("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.

   Agree: 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.

   Agree: 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 to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

   Agree: Agree

Provider Initial: JC
Date: 07/18/2025

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section I: General - All Data *(Continued)*

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.

   Agree: 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.

   Agree: 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.

   Agree: 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 uploaded data 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 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?

   Agree: 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).

   Agree: 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.

   Agree: Agree

Provider Initial: JC
Date: 07/18/2025

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

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.

   Agree: 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.

   Agree: Agree

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

   Agree: 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.

   Agree: Agree

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

   Agree: 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.

   Agree: 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 (See Page 2, Item 9).

   Agree: Agree

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

   Agree: Agree

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

   Agree: Agree

Provider Initial: JC
Date: 07/18/2025

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

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.

   Agree: Agree

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

   Agree: Agree

3. Vendors cannot sell student information.

   Agree: Agree

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

   Agree: Agree

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

   Agree: Agree

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

   Agree: Agree

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

   Agree: Agree

Provider Initial: JC

Date: 07/18/2025

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

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.

Section IV: Audit and Compliance Oversight (*Continued*)

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

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.

Provider Initial: JC
Date: 07/18/2025

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

EXHIBITS

Section 1.6: External Security

Peachjar application and data are hosted within Amazon Web Services.
- Firewalls and IDS/IPS are standardly employed within the AWS VPC.
- All data is housed within AWS infrastructure and secure within VPCs.
- All physical and environmental controls are governed by Amazon Web Services best practices. Amazon oversees physical access management and intrusion detection response.

Section 1.7: Internal Security

The Peachjar platform has password protected access to data via external and internal web portals. Only authorized staff and users can access the system and controls are in place within the application to ensure users see only their data. Peachjar's InfoSec Policy and internal training emphasizes the importance of confidentiality and securing PII.

Peachjar restricts data access to the IT specialist(s) assigned to support your account. Only employees that have completed a security briefing and acknowledgment are given access to the database and the number of employees with this access is always kept to the essential minimum.

Parent email addresses and their associated school and grade level are securely transferred from the district SIS to your Peachjar server using SFTP to encrypt data. All active sessions use HTTPS to provide bi-directional encryption of communications between client and server.

Data is backed up daily. Backups are retained for up to 30 days before deletion. Should a catastrophic failure occur Peachjar is able to redeploy the application from repositories and restore databases from backups.

Section II.2: Exporting of Student-Created Content

No student-created content is present on Peachjar's systems.

Provider Initial: JC
Date: 07/18/2025

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

EXHIBITS

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

Parents/guardians are able to access their Peachjar accounts and update information on their profile. They can review and edit:
- Email address (parent/guardian)
- School
- Grade level

Section II.5: Securing Student Data

The Peachjar platform has password protected access to data via external and internal web portals. Only authorized staff and users can access the system and controls are in place within the application to ensure users see only their data. All data is encrypted in-transit (SSL/TLS) and at-rest (AES-264).

Peachjar monitors for security threats and leverages existing AWS resources to do so. Logging occurs on a 24x7x365 basis.

Peachjar's InfoSec Policy and internal training emphasizes the importance of confidentiality and securing PII.

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

Peachjar does not collect or access any personally identifiable student information, as defined under FERPA. Specifically, Peachjar only accesses parent/guardian email addresses, the associated school and grade level. FERPA refers to this as "directory information." (Section 99.3).

All data is encrypted and secured behind access controls and firewalls. Peachjar staff are trained on FERPA regulations and their responsibilities. Parents/guardians are able to update the information stored on their profile. Procedures and measures are in place to de-identify data upon request. Peachjar will not share nor sell parent/guardian email addresses or associated data to any third party.

Section III.5: How Student Data is Protected:

Peachjar uses industry standard security safeguards to protect information against loss or theft, as well as unauthorized access, disclosure, copying, and use.

Peachjar's InfoSec Policy and internal training emphasizes the importance of confidentiality and securing PII.

Peachjar will not share, sell, or otherwise disclose parent/guardian email addresses or any other confidential information to any third party where not required by law.

Provider Initial: JC
Date: 07/18/2025

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

ARTIFICIAL INTELLIGENCE (AI) ADDENDUM

1. AI Usage Limitations and Ownership

1.1. The Service Provider shall not use or reproduce Student Data for Artificial Intelligence (AI) training, model development, 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, the Provider shall notify the District in writing prior to deployment.

2.2. The Provider must disclose the types of AI 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 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. These audits shall demonstrate the Provider's commitment to promoting equitable outcomes and addressing systemic bias, as emphasized in 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.

Provider Initial: JC
Date: 07/18/2025

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

5. Prohibited Uses of AI

5.1. The Provider shall not:

- Use AI to generate synthetic or inferred Student Data.
- Develop behavioral profiles for marketing or advertising.
- Engage in predictive analytics that may result in automated decision-making affecting students without human oversight.
- 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

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

- Ensure students can download or export that content.
- Retain no ownership or claim over AI-assisted student work.
- Maintain logs of AI interactions in accordance with FERPA.
- 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. The Provider shall maintain and make publicly available a free tool that enables users to verify whether content was generated by AI. This tool shall:

- Provide provenance data (excluding personal data).
- Support multiple content formats.
- Accept user feedback to support continuous improvement.

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

- The Provider's name.
- Identification of the AI system used.
- The creation date and time.
- 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.

Provider Initial: JC
Date: 07/18/2025

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

8. Definitions

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

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

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

9. Compliance with State Advisory Guidelines

9.1. 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.

Provider Initial: JC
Date: 07/18/2025

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

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 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.

Provider Initial: JC
Date: 07/18/2025

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

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 made in relation to the incident and shall make such records available to the District upon request.

Provider Initial: JC
Date: 07/18/2025

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

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.

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.

Provider Initial: JC

Date 07/18/2025

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

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.

Service Provider		**Roseville City School District**	
Joe Cremer		Laura Assem	
Authorized Representative Signature		*Authorized Representative Signature*	
Date:	07/18/2025	**Date:**	07/18/2025
Name:	Joe Cremer	**Name:**	Laura Assem
Title:	Director, Product and Engineering	**Title:**	Executive Director, Technology Services
Email:	joecremer@peachjar.com	**Email:**	lassem@rcsdk8.org

8697 La Mesa Blvd., Suite C
La Mesa, CA 91942

peachjar

ADDENDUM TO DATA PRIVACY AGREEMENT

This Addendum ("Addendum") is entered into by and between Peachjar, Inc. ("Service Provider") and Roseville City School District ("District"), collectively referred to as the "Parties," effective as of July 18, 2025.

This Addendum clarifies the use of de-identified and aggregated data under the existing agreement ("Agreement") between the Parties, specifically addressing data originally collected under the Agreement pertaining to Roseville City School District. The terms herein supplement and amend the terms of the Agreement and in the event of a conflict between the Agreement and this Addendum, the Addendum controls.

Terms:

1. **Permanent Deletion Obligation:** Consistent with the Agreement, Service Provider shall permanently delete all student covered information relating to Roseville City School District as required.
2. **Permissible Use of De-identified Data:** Notwithstanding Section 1 above, the Parties acknowledge and agree that Service Provider may retain and use de-identified student covered information as permitted under California Senate Bill 1177 (Student Online Personal Information Protection Act), specifically:
    a. Service Provider may use de-identified student covered information:
        i. Within the Service Provider's site, service, or application, or other sites, services, or applications owned by the Service Provider, to improve educational products.
        ii. To demonstrate the effectiveness of the Service Provider's products or services, including in marketing materials, provided such data remains de-identified and does not reveal any individual student's identity.
        iii. Service Provider may share aggregated de-identified student covered information with third parties for the development and improvement of educational sites, services, or applications.
3. **Definition of De-identified Data:** For purposes of this Addendum, "de-identified student covered information" shall mean information that cannot reasonably be used to identify an individual student and is consistent with the de-identification standards outlined in SB 1177.
4. **No Impact on Student Privacy Obligations:** This Addendum does not alter or diminish the Service Provider's obligations under the Agreement or applicable law to protect student covered information and maintain its confidentiality and security

Peachjar, Inc. Security Incident Plan

Version 1.1

Table of Contents

Introduction

Statement of Intent

This Security Incident Plan describes the policies and procedures of Peachjar, Inc. (also referred to as “Peachjar”, “Company”, “we”, “our”, or “us”), as well as process-level plans for identifying and recovering from a security incident. The primary purpose of this document is to ensure physical safety of people, systems, and data.

Our mission is to ensure data security, information system operation, data integrity and availability, and business continuity.

Policy Statement

Management has approved the following policy statement:

- The Company comprehensive Security Incident Plan shall be reviewed annually. A risk assessment shall be undertaken periodically to determine the requirements for the Security Incident Plan.
- Management responsibilities and procedures should be clearly established to ensure a quick, effective, and orderly response to Security Incidents.
- The objectives for Security Incident management should be agreed upon with management, and it should be ensured that those responsible for Security Incident management understand the organization’s priorities for handling Security Incidents.
- Personnel and contractors using the organization’s information systems and services are required to note and report any observed or suspected security weakness in systems or services.
- Security Events should be assessed and it should be decided if they are to be classified as Security Incidents.
- Security Incidents should be responded to in accordance with documented Incident Response procedures.
- Security Events should be reported through appropriate management channels as quickly as possible.
- In the event of a Security Incident, data controllers, government bodies and other necessary parties should be notified in a reasonable timeframe, and in compliance with regulatory and other applicable requirements and guidance.
- Knowledge gained from analyzing and resolving Security Incidents should be used to reduce the likelihood or impact of future incidents.
- Procedures should be defined and applied for the identification, collection, acquisition, and preservation of information, which can serve as evidence.

- Awareness should be provided on topics such as:
    - The benefits of a formal, consistent approach to Incident Management (personal and organizational);
    - How the program works, expectations;
    - How to report Security Incidents, who to contact; and,
    - Constraints imposed by non-disclosure agreements.
- Communication channels should be established well in advance of a Security Incident. Include all necessary parties in relevant communication:
    - Security Incident response team members
    - Senior Management
    - Company Personnel

Objectives

The principal objective of the Security Incident program is to Develop, Test and Document a well-structured and easily understood plan which will help the Company recover as quickly and effectively as possible from an unforeseen Security Incident. Employees will fully understand their duties in implementing such a plan that the operational policies are adhered to within all planned activities.

Definition of a Security Incident

Data Breach means a Security Incident that directly impacts sensitive data or personal information.

Security Event means an identified occurrence of a system, service or network state indicating a possible breach of Information Security Policy, a possible exploitation of a security vulnerability or security weakness or a previously unknown situation that can be security relevant.

Security Incident means a single or series of unwanted or unexpected Security Events that compromise business operations with an impact on Information Security.

Common Incident Types

Incident Type	Type Description
Unauthorized Access	When an individual or entity gains logical or physical access without permission to a company network, system, application, data, or other resource.
Denial of Service (DoS, DDoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources.
Malicious Code	Successful installation of malicious software (e.g., a virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.
Improper or Inappropriate Usage	When a person violates acceptable computing policies, including unauthorized access or data theft.
Suspected PII Breach	An incident where it is suspected that Personally Identifiable Information (PII) has been accessed.
Suspected loss of Sensitive Information	An incident that involves a suspected loss of sensitive information (not PII) that occurred because of Unauthorized Access, Malicious Code, or Improper (or Inappropriate) use, where the cause or extent is not known.

Scope

The Peachjar Security Incident Plan takes all of the following areas into consideration:

- Server Infrastructure
- Data Storage and Backup Systems
- Data Output Devices
- End-user Computers
- Organizational Software Systems
- Database Systems

Security Incident Response Teams & Responsibilities

In the event of an incident, different roles will be required to assist in the effort to assess, react, recover and learn from the incident. The different groups and their responsibilities are as follows across the overall Incident Response Team:

Security Incident Response Team

- Security Incident Coordinator
- Legal
- IT
- Finance
- Human Resources
- Public Relations/Communications
- Privacy/Regulatory/Compliance
- Senior Management

Security Incident Coordinator

The Security Incident Coordinator is responsible for coordinating all decisions related to the security incident. This person's primary role will be to guide the recovery process and all other individuals involved in the recovery process will report to this person in the event that a Security Incident occurs at Peachjar, regardless of their department and existing managers.

Role and Responsibilities

- Contact the members of the Incident Response Team to initiate the response plan
- Determine which Incident Response Team members play an active role in the investigation
- Escalate to executive management as appropriate
- Contact auxiliary departments as appropriate
- Monitor progress of the investigation
- Ensure evidence gathering, chain of custody, and preservation is appropriate
- Be the single point of contact for other team members
- Present to the Incident Response Team on the state of the Security Incident and the decisions that need to be made
- Prepare a written summary of the Security Incident and corrective action taken

Legal

The legal team that will oversee the legal response for the Security Incident. This includes ensuring that proper disclosure laws are properly followed where proper communication is warranted with affected parties and/or authorities. Furthermore, they will help with coordinating the level of response and internal communications protocol, in order to ensure process and information surrounding the Security Incident generates the proper artifacts to protect sensitive data, customers, vendors and the company overall.

Role & Responsibilities

- Coordinate communication with data breach and general counsel
- Coordinate activities between business areas and other departments (e.g., Human Resources, if necessary)
- If necessary, notify the appropriate authorities (e.g., state attorneys general, FBI, etc.)
- Coordinate with Public Relations on the timing and content of notification to individuals
- Follow approved procedures and timelines for any notice of unauthorized access to personal information about individualsIssue a “communications protocol” memo advising personnel involved in the Security Incident response regarding proper communications (i.e., what not to put in writing, e.g., admissions, blame, speculation, opinions, etc.)
- Issue a “litigation” hold memo, when appropriate, to ensure information is retained for litigation purposes

IT

The IT Team will be responsible for evaluating if a Security Incident has occurred and the extent of the Security Incident. They will also coordinate data backups as necessary and any system failover procedures in order to protect data as necessary. In the event that third party forensic teams are warranted in order to contain and investigate the extent of a breach, they will help coordinate and unblock resources to drive resolution as quickly as possible.

Role & Responsibilities

- Take the lead in investigation, evidence preservation, and remediation
- Ensure that secondary servers located in standby are kept up-to-date with system patches
- Ensure that secondary servers located in standby are kept up-to-date with application patches

- Ensure that secondary servers located in standby are kept up-to-date with data copies
- Ensure that all of the backup servers in the standby abide by Peachjar's server policy
- Manage and coordinate any tools, hardware, and systems required for system backup and redundancy
- Ensure that proper security protocols are in place and leveraged across the organization to limit risk
- Coordinates any third party resources leveraged to evaluate, address and/or prevent a security incident

Finance

The Finance Team will be responsible for coordinating payments related to expenses to address any security related incidents. They will engage with the Security Incident Coordinator to authorize remediation steps that will require a financial cost to the Company.

Role & Responsibilities

- Approves any payments (e.g., ransom) and expenses for service providers (e.g., forensics, PR firm, outside legal counsel, etc.)

Human Resources

Human Resources's primary goal will be to provide employees with the information that they need to keep internal teams informed about any actions necessary across the organization.

Role & Responsibilities

- Work with the IT to identify the extent of the Security Incident in the event of a malicious action or theft committed by internal staff
- Work with Legal to determine if the Security Incident warrants notification to employees or other further action

Public Relations/Communication

This will be the team responsible for all communication during a Security Iincident. Specifically, they will communicate with Peachjar's employees, clients, vendors and suppliers, banks, and even the media if required.

Role & Responsibilities

- Coordinate with the CEO and Legal on the timing, content and method of notification
- Prepare appropriate responses to media, customer, and/or employee; and have the CEO and Legal approve prior to distribution
- Communicate the occurrence and impact of a Security Incident to all Peachjar's employees
- Communicate the occurrence and impact of a Security Incident to authorities, as required
- Communicate the occurrence and impact of a Security Incident to all Peachjar's partners
- Communicate the occurrence and impact of a Security Incident to all Peachjar's clients
- Communicate the occurrence and impact of a Security Incident to all Peachjar's vendors
- Communicate the occurrence and impact of a Security Incident to media contacts, as required

Senior Management

The Senior Management Team will make any business decisions that are out of scope for the other teams. Decisions such as replacing major architecture elements for the platform, incurring high financial costs to minimize long term impact and risk, etc. should be made by the Senior Management Team. The Security Incident Coordinator will ultimately report to this team.

Role & Responsibilities

- Ensure that the Security Incident Coordinator is held accountable for their role
- Assist the Security Incident Coordinator in their role as required
- Make decisions that will impact the Company. This can include decisions concerning:
    - Rebuilding of data centers
    - Significant hardware and software investments and upgrades
    - Financial and business decisions necessary to manage disaster resolution and impact

Security Incident Response Process Overview

- **Detect, Investigate and validate** the Security Incident
- **Preserve evidence**

- **Activate response team**
    - Security Incident Coordinator assembles the team and communicates what is known
- **Advise legal counsel**
    - Use outside counsel because attorney-client privilege may not always exist with in-house counsel (in-house often wears business hat, and communication is not privileged)
    - Identify notification requirements based on scope of the Security Incident (see notify stakeholders)
- **Complete forensics investigation**
    - Identify and determine scope and composition of the Security Incident
        - Data types: personal, credit card, employee, trade secrets, banking, intellectual property, login credentials, account numbers, etc.
        - Which files and servers were accessed
        - Which physical assets are missing
    - Preserve evidence of the Security Incident (don't delete files or wipe hard drives)
    - Quarantine, shut down, isolate, disinfect, eradicate, etc.
    - If outside forensics investigator used, hire through outside counsel to maintain attorney-client privilege
    - Vendor investigation: If vendor was breached, get the facts, review contractual obligations, get commitment to cooperate
- **Notify stakeholders**
    - Determine notification requirements (legal will handle)
        - Affected individuals
            - Determine in which states affected individuals reside
            - Determine whether credit monitoring or credit freeze services are required or advisable
        - Data owners (e.g., customer)
        - Law enforcement, state attorney general, consumer agency, as required
    - Prepare notification letters, if required (legal will handle)
    - Management
    - Insurance carrier
- **Coordinate communications** with PR team (and legal)
- **Recover and close** out the problem that led to the Security Incident
- **Complete incident retrospective**
    - Draft report with findings and overall learnings
    - Prevent future incidents through training, process change and system updates

Dealing with a Security Incident

Detect, Investigate and Validate

Given that a Security Incident can manifest itself through various channels it is critical that the business is leveraging both system monitoring tools and user reported information in order to support the initial detection of a Security Incident. This includes but is not limited to the detection points below:

- System alarms and network monitors
- Anti-virus software
- Internal users
- End users
- 3rd party vendors

Internal teams will be trained to report any suspicious activity through the #info-security channel in Slack or directly to the IT lead.

IT will determine whether the Security Incident or suspected Security Incident is serious enough to warrant full incident response plan activation. In the event that the Security Incident is tied to internal user behavior, legal and HR teams will be included to ensure that proper investigation measures are completed. Others will assist in acquiring information, preserving evidence, and providing additional resources as deemed necessary by the IT, Legal, HR or other Security Incident Response Team members throughout the investigation. If a valid Security Incident is detected it will trigger the preservation of evidence and activation of the Security Incident Response Team. In the event of a ransomware request all communication must immediately be funneled through Legal.

Owners: IT, Legal, HR

Preserve Evidence

After a Security Incident has been confirmed the first step is to preserve as much of the evidence as possible. This may include any system based activity logs tracking log in/log out and related read/write/copy/delete actions that may be connected to the activity. In the event of theft of physical hardware, all details around the inventory affected will be documented along with the last known location and owner. Authorities will be contacted as warranted and advised by Legal.

Owner(s): IT, Legal, HR

Activate Response Team

After a Security Incident has been identified the Security Incident Coordinator is alerted. They will subsequently alert all the leads across the supporting teams. A new Slack channel will be created along with the link to a standing virtual meeting that can be leveraged throughout the Security Incident as necessary. **The Slack channel will be used as a resource coordination tool but not as a place to collect, post, store or validate any evidence or actions connected to the Security Incident.**

All communication will be coordinated through the Public Relation/Communication team and discussion on progress will be maintained through the virtual meeting. **Transcripts are not turned on for the meeting** as notes will be kept separately and coordinated through the Security Incident Coordinator.

IT will set up the proper repository where evidence, notes and other artifacts pertaining to the Security Incident will be collected. Access will be provided as necessary in order to manage the response.

Owner(s): Security Incident Coordinator, IT, Legal, HR

Advise Legal Counsel

As the incident is launched by the Incident Security Response Team it is critical that proper legal steps are taken per the Security Incident type and scope. In order to ensure that we manage any given Security Incident in accordance with the proper communication and disclosure requirements, we will reach out to external legal counsel to help coordinate the response. External counsel is also important because attorney-client privilege may not always exist with in-house counsel (in-house often wears business hat, and communication is not privileged).

- **Reporting Requirements**
    - To assess whether a Security Incident must be reported, Personnel should consider whether there are indications that:
        - Information was used by unauthorized Personnel or Third Parties;
        - Information has been downloaded or copied inappropriately from computer systems or equipment;

        - Equipment or devices containing Information have been lost or stolen;
        - Equipment or devices containing Information have been subject to unauthorized activity (e.g., hacking, malware).
        - Personal information has been publicly exposed.
        - In addition, the following situations should be considered for Security Incident reporting:
        - Ineffective security controls;
        - Breach of information integrity, confidentiality or availability expectations;
        - Human errors (innocent or otherwise);
        - Non–compliance with policies or standards;
        - Breaches of physical security arrangements;
        - Uncontrolled systems changes;
        - Malfunctions of software or hardware;
        - Access violations.

Owner(s): Legal

Complete Forensics Investigation

In parallel to all other Security Incident management steps the proper investigation efforts will continue in parallel in order to identify, isolate, gather evidence and eliminate the security threat. This work is contained in the steps and efforts below:

- **Identify Scope**
    - Date, time, duration and location of Security Incident
    - How the Security Incident was discovered, who discovered the Security Incident and any known details surrounding the Security Incident, such as:
        - Method of intrusion;
        - Entry or exit points;
        - Paths taken;
        - Compromised systems;
        - Whether data was deleted, modified or viewed; and
        - Whether any physical assets are missing
    - Details about the compromised data, including:
        - a list of affected individuals, type (for example, employee, vendor or customer); and state/country of residence
        - data fields (including all fields of personal information);
        - number of records affected; and
        - whether any of the data was encrypted and if so, what fields

    - In the event of ransomware, determine type and strain/variant of ransomware. Look for a pattern of encryption, request for payment, file names, and whether it is a new strain.
        - Determine if the decryption tool for that variant is publically available (search web, ask FBI). Older ransomware versions often have the decryption key published. Sometimes the FBI can identify a key based on the ransomware version.
- **Preserve evidence**
    - Preserve all data and evidence, including forensic evidence, collected in the event of any later legal or regulatory action. The business should also keep a log of actions taken during the investigation.
- **Quarantine**
    - Ensure all intrusion entry or exit points are closed off
        - Compromised logins
        - Compromised systems
    - Determine if an affected system has accessed other systems and isolate those systems/access points.
    - If a system is effectively quarantined, do not wipe or disinfect that computer until instructed to do so, as it may be needed for forensic review.
    - If physical assets are missing, remotely remove access to any systems or logins connected to the missing asset.
    - Evaluate backups and what recovery options exist to get systems back and functional.
    - Post quarantine, run scans across all computers/systems.
- **Third Party Investigators**
    - If an outside forensics investigator is used, hire through outside counsel to maintain attorney-client privilege.
- **Vendor investigation**
    - If vendor was breached, get the facts, review contractual obligations, get commitment to cooperate.
    - Remove any vendor access where appropriate in order to contain the incident.

Owner(s): IT

Notify Stakeholders and Coordinate Communications

Stakeholder notification can occur with the approval of legal and the Senior Management Team. This will start with validating what types of disclosure requirements may be needed based on the forensic analysis completed by the IT team. Prior to any external communication, internal teams must be instructed with

proper response templates in order to ensure a standardized and consistent approach to impacted stakeholders.

- **External Notification Requirements**
    - Determine notification requirements (legal will handle)
        - Affected individuals
            - Determine in which states affected individuals reside
            - Determine whether credit monitoring or credit freeze services are required or advisable
        - Data owners (e.g., customer)
        - Law enforcement, state attorney general, consumer agency, as required
    - Prepare notification letters, if required (legal will handle)
    - Contact insurance carrier as necessary
    - Legal should retain and be copied on all communication with forensics firms to maintain attorney-client privilege.
- **Internal Notification Requirements**
    - HR and Legal will determine if the Security Incident warrants notification to employees or other further action.
    - Legal and HR will, where warranted, issue a “communications protocol” memo advising personnel involved in the Security Incident response regarding proper communications (i.e., what not to put in writing, e.g., admissions, blame, speculation, opinions, etc.)
    - Legal and HR will, where warranted, issue a “litigation” hold memo, when appropriate, to ensure information is retained for potential litigation purposes.

Owner(s): Legal, HR, IT Public Relations/Communication

Post Security Incident Processing

Complete Security Incident Retrospective

During a review of each team’s relevant areas, they must assess any areas where further Security Incidents can be prevented and take the necessary means to protect Peachjar’s assets. Any necessary repairs or preventative measures must be taken to protect the organization; these costs must first be approved by the Senior Management Team.

All teams will be required to create an initial report on the damage and provide this to the Security Incident Coordinator within **2 weeks** of the initial Security Incident.

This includes all actions taken and summarizing any and all costs incurred. Future prevention efforts along with priority and timing must also be included.

The Security Incident Coordinator will pull details together across each team. This will be summarized in a report that includes:

- Date and time of the Security Incident
- Scope and impact
- Mitigation steps, dates and outcomes
- Communication dates and content provided
- Costs incurred
- Lessons learned
- Prevention options moving forward

Owner(s): Security Incident Coordinator

Cost Factors

Insurance
As part of the Company's Security Incident recovery strategy, a number of insurance policies have been put in place. . Usage and impact of these policies must be evaluated.

Financial Assessment
The Security Incident Response Team shall prepare an initial assessment of the impact of the Security Incident on the financial affairs of the Company.

Financial Requirements
The immediate financial needs after assessing the damage must be addressed. These can include:

- Cash flow position
- Temporary borrowing capability
- Upcoming critical payments such as payroll, etc.
- Availability of credit cards to pay for supplies and services required post-disaster

Legal Actions
The legal team will review the aftermath of the Security Incident and decide whether there may be legal actions resulting from the event.

IT Infrastructure

Assessment of IT infrastructure impacts and potential costs in altering the architecture during or after the Security Incident. This assessment must include:

- Loss of Client Data estimation. (Period and approx. Size of data)
- Loss of Infrastructure

Process Impact
If operational processes must change as part of the Security Incident recovery and response, financial and staffing costs must be assessed accordingly.

Maintenance

The Security Incident Plan will be updated annually or any time a major system update or upgrade is performed, whichever is more often. The Security Incident Coordinator will be responsible for updating the entire document, and so is permitted to request information and updates from other employees and departments within the organization in order to complete this task.

Maintenance of the plan will include (but is not limited to) the following:

- Ensuring that all team lists are up to date
- Reviewing the plan to ensure that all of the instructions are still relevant to the organization
- Making any major changes and revisions in the plan to reflect organizational shifts, changes and goals
- Ensuring that the plan meets any requirements specified in new laws
- Other organizational specific maintenance goals

During the maintenance periods, any changes to the Security Incident Response Teams must be accounted for. If any member of a Security Incident Response Team no longer works with the Company, it is the responsibility of the Security Incident Coordinator to appoint a new team member.

Testing

Peachjar is committed to ensuring that this plan is functional. The Security Incident Plan should be tested annually in order to ensure that it is still effective. Testing the plan will be carried out as follows:

- **Walkthroughs -** Team members verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or

other weaknesses. This test provides the opportunity to review a plan with a larger subset of people, allowing the lead to draw upon a correspondingly increased pool of knowledge and experiences. Staff should be familiar with procedures, equipment, and systems.

- **Simulations -** A Security Incident is simulated so normal operations will not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms and documentation should be thoroughly tested in a simulation test.

Any gaps in the plan that are discovered during the testing phase will be addressed by the Security Incident Coordinator as well as any resources that he/she will require.