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

Synovia Solutions LLC
"Service Provider" or "Vendor"

("Service Provider" or "Vendor") on

06/11/2026
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 cannot create content in this system.

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:

Not Applicable

Breach Notification Not Applicable

Synovia will share our incident response plan with Roseville City School District subject to a signed NDA between both parties. Roseville City School District will be responsible for notifying affected parents, legal guardians, or eligible students when student records are unauthorizedly disclosed.

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 SP 800-53, NIST Cybersecurity Framework (NIST CSF)

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

Synovia can provide reasonable evidence of security controls and independent assurance through its SOC 2 Type 2 certification report, which can be shared under a fully executed mutual Non-Disclosure Agreement.

Security controls and ongoing testing
Synovia performs periodic internal vulnerability scans and external web application scans, prioritizes findings for remediation, and drives remediation through regular touchpoints with Production Operations/ProdOps (weekly/ biweekly).
A third party is engaged to conduct penetration testing and vulnerability scanning, with issues disclosed to management in accordance with Synovia's patch management process.
Network protections (including IDS preference)
Network Intrusion Detection/Prevention Systems (NIDS/NIPS) are employed.
Synovia confirms security standards/baseline configurations/patching/access control/strong passwords for network devices including firewalls, switches, routers, and wireless access points.
Guest access must be logically separated from the Synovia network via a demilitarized zone (DMZ), firewall, or other access control, with monitoring performed on all guest activity.
Data is encrypted in transit and at rest; encryption at rest uses AES 256-bit and encryption in motion uses TLS 1.2+; the solution supports FIPS 140-2 Level 1 security. In addition, we use a WAF and network firewall.
Devices use industry best practices with a proprietary message format.
Synovia can provide SAML 2.0 sign-in through an identity provider.
Synovia's security policies applicable to outsourcing and vendor connections include Data Management Policy, Access Control Policy, System Security Policy, and Encryption Policy; vendor connections are restricted to legitimate business needs and minimum necessary access, with required identity verification mechanisms for authorized employees and change confirmation.

Section 1.7: Internal Security

Synovia can provide independent assurance and supporting evidence of security controls through its SOC 2 Type 2 certification report under a fully executed mutual NDA, and it conducts periodic internal vulnerability scans and external web application scans with findings prioritized for remediation and driven to completion through regular Production Operations/ProdOps touchpoints. Real-time threat detection is also performed internally.
Synovia's operating model anticipates that customer-facing issue intake is handled through a front-end gathering process provided by the client, and Synovia then uses the provided information to troubleshoot and resolve technical issues via its support organization. Complaints are ingested and escalated through account and customer personnel.
Role-based access control (RBAC) is enforced so users only access authorized data, with a Security and Compliance team responsible for data protection, privacy controls, secure data handling, encryption, and access governance leveraging best practices within AWS.
Encryption and cryptographic standards: Data is encrypted in transit and at rest; encryption at rest uses AES 256-bit and encryption in motion uses TLS 1.2+; the solution supports FIPS 140-2 Level 1 security.
Synovia is hosted in AWS and uses geographically diverse backups, leveraging multiple geographically distributed cloud regions to support durability. Synovia’s Data Management Policy requires at least weekly backups and requires that system devices and data have backups scheduled for at least 90 days and archived.
For confidential data, paper/documents, cross-cut shredding is required; for removable media (CDs/DVDs), physical destruction is required; and physical hardware must be wiped and physically destroyed.

Section II.2: Exporting of Student-Created Content

Not Applicable. Students cannot create content inside this system.

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

Synovia’s Privacy Policy describes GDPR rights that allow users to review and request corrections to their personal data, including the right to find out what information Synovia holds about them, obtain a copy of their personal data, and request the correction or deletion of their personal data. These rights can be exercised by contacting Synovia using the contact information provided in the policy, submitting the form available via the “Contact Us” hyperlink, or emailing privacy@CalAmp.com.

Section II.5: Securing Student Data

Yes—Synovia can provide evidence and supporting documentation describing how data is kept secure and confidential, including encryption, access controls, and independent assurance.
Evidence Synovia can attach/provide
- SOC 2 Type 2 certification report (shareable under a fully executed mutual NDA).
- Data privacy and data retention policies (providable under mutual NDA).
- CalAmp Privacy Policy (https://www.calamp.com/privacy-policy/).
- Key security and governance policies (Vendor Risk Management Policy, Access Control Policy, Data Management Policy).
How confidentiality and security are implemented
- Encryption: Data is encrypted at rest using AES 256-bit and encrypted in transit/in motion using TLS 1.2+.
- Access controls: Synovia implements strict access controls to internal systems.
- Confidential data handling controls: Users must use strong passwords and multi-factor authentication (where available) for applications handling confidential data.

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

To the extent applicable, Synovia aligns with FERPA requirements when handling student data.

Section III.5: How Student Data is Protected:

Yes—Synovia can provide evidence and supporting documentation describing how data is kept secure and confidential, including encryption, access controls, and independent assurance.
Evidence Synovia can attach/provide
- SOC 2 Type 2 certification report (shareable under a fully executed mutual NDA).
- Data privacy and data retention policies (providable under mutual NDA).
- CalAmp Privacy Policy (https://www.calamp.com/privacy-policy/).
- Key security and governance policies (Vendor Risk Management Policy, Access Control Policy, Data Management Policy).
How confidentiality and security are implemented
- Encryption: Data is encrypted at rest using AES 256-bit and encrypted in transit/in motion using TLS 1.2+.
- Access controls: Synovia implements strict access controls to internal systems.
- Confidential data handling controls: Users must use strong passwords and multi-factor authentication (where available) for applications handling confidential data.

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

Synovia - SOC 3 Report 2025 - Final.pdf

Roseville City School District DPA - Synovia Exceptions v. 1 06-08-2026.docx

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

5. Prohibited Uses of AI

The Provider shall 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. 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:

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 permanent 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. 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.

Service Provider Signature	**Date Signed**
Nicholas Nowak	06/08/2026 03:38 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

Nicholas Nowak

Date Signed

06/08/2026 03:41 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

Nicholas Nowak

Service Provider

Date

06/11/2026 08:21 am

Service Provider

Name

Nicholas Nowak

Service Provider

Title

Senior Software Manager

Service Provider

Email (Service Provider)

nnowak@calamp.com

Service Provider

Date

06/11/2026 07:18 am

Roseville City School District

Name

Laura Assem

Roseville City School District

Title

Executive Director, Technology Services

Roseville City School District

Roseville City School District Data Privacy Agreement
Synovia/Vendor Solutions LLC's Exceptions to Data Incident Notification Addendum

1. **Data Incident Notification**. Synovia/Vendor will notify Customer/LEA without undue delay and within a commercially reasonable timeframe consistent with applicable law after confirming a Data Incident. Synovia/Vendor will cooperate with Customer/LEA's reasonable requests, provided Synovia/Vendor retains control over its incident response and such cooperation does not conflict with legal or security obligations.

2. **Notification to Individuals and Authorities**. Synovia/Vendor will provide notifications only where required by applicable law. The parties will cooperate in good faith to determine appropriate timing and content. Synovia/Vendor will not be required to notify where no legal obligation exists or where risk of harm is not material.

3. **Credit Monitoring**. Synovia/Vendor will provide credit or identity monitoring services only where legally required and where the incident is directly caused by Synovia/Vendor's breach. Any such services will be commercially reasonable in scope and duration and not exceed twelve (12) months.

4. **Regulatory Notification**. Synovia/Vendor will comply with applicable legal requirements for regulatory notification but will not be obligated to provide notices beyond those required by law.

5. **Records and Audit**. Synovia/Vendor will maintain records consistent with its internal policies. Any access by Customer/LEA will be subject to confidentiality obligations and reasonable limitations.

6. **Confidentiality**. Synovia/Vendor may disclose incident details as required by law or to its insurers, advisors, or incident response providers. Otherwise, disclosures will be coordinated with Customer/LEA where reasonably practicable.

7. **Subcontractors**. Synovia/Vendor will require subcontractors to maintain commercially reasonable data protection obligations and will remain responsible only to the extent of its control over such subcontractors.

8. **Cooperation**. Synovia/Vendor will provide commercially reasonable cooperation. Customer/LEA shall reimburse Synovia/Vendor for extraordinary support beyond standard obligations.

9. **Financial Responsibility**. Each party is responsible for its own acts or omissions. Synovia/Vendor's liability shall be subject to the limitation of liability in the Agreement.

10. **Indemnity**. Synovia/Vendor will indemnify Customer/LEA only for third-party claims directly caused by Synovia/Vendor's breach of data security obligations. Indemnity excludes Customer/LEA acts, misuse, and third-party causes. Liability is subject to caps and defense control provisions.

11. **Limitation of Liability**. Synovia/Vendor's total liability for Data Incidents shall be subject to the Agreement limits. Synovia/Vendor shall not be liable for indirect or consequential damages or for incidents caused by factors outside its control.

12. **Security Standard**. Synovia/Vendor will maintain commercially reasonable safeguards but does not guarantee that Data Incidents will never occur.