

**RIVERSIDE COUNTY OFFICE OF EDUCATION  
3939 Thirteenth Street  
Riverside, California 92501**

**MEMORANDUM OF UNDERSTANDING FOR DATA SHARING SERVICES**

This Agreement is entered into by and between the Riverside County Superintendent of Schools, hereinafter referred to as “RCOE”, and Perris Union High School District, hereinafter referred to as “LEA”, each being a “Party” and collectively the “Parties”.

**WHEREAS**, RCOE and LEA enter into this MOU to facilitate the mutual sharing of data and establish responsibilities between the Parties; and

**WHEREAS**, the Parties wish to protect the privacy of pupil records, and to comply with any applicable privacy statutes, including the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 C.F.R. Part 99, as amended; “FERPA”); California Education Code § 49073.1; the Student Online Personal Information Protection Act (California Business and Professions Code § 22584; “SOPIPA”); California Civil Code § 1798.29; and California Government Code § 6250 et seq.; and

**WHEREAS**, the purpose of this MOU is to set forth the rights and responsibilities of RCOE and LEA with respect to data collected or retained by LEA or by RCOE pursuant to this MOU.

**NOW THEREFORE**, in consideration of the terms and conditions hereof, including the recitals, the Parties agree as follows:

**1. Role of RCOE**

RCOE shall provide services designed to assist LEA with certain requirements and mandates for managing or reporting on data collected by LEA, potentially including the integration of data between disparate systems, and staff and pupil records, which include any information that is directly related to a student that is maintained by LEA or acquired directly through the use of instructional software or applications assigned to a student by a teacher or other LEA employee (collectively, “Data”). Services rendered under this MOU shall be referred to as “Data Services”.

1.1 If LEA requests any additional services from RCOE not encompassed by the Data Services, the Parties may agree to a fee for the performance of these “Additional Services,”. Such Additional Services, as agreed to by the Parties separately in writing, may include those relating to Galaxy Reports, Microstrategy Reports, Student Information Systems, Data Hosting Services, annual audits, annual trainings for staff, assistance in security of the LEA maintained systems, and other administrative services with respect to the LEA’s data systems, such as collection, extraction or backup of Data on behalf of the LEA.

**2. Responsibilities of RCOE**

RCOE will provide any services it delivers in a timely and professional manner.

2.1 RCOE will assist with the automation of any processes required for the exchange of Data between the Parties to the extent possible.

2.2 RCOE will ensure any systems it develops with such Data to serve the needs of LEA or public agencies will have appropriate levels of security, as further detailed in Section 12 (Data Security) of this MOU.

2.3 RCOE shall help ensure LEA Data can only be viewed or accessed by agencies legally allowed to do so, and as agreed upon by LEA and RCOE.

2.4 Should it be deemed necessary, RCOE will specify and assist in allowing network access to resources, in a controlled and secure manner.

### 3. LEA Rights and Responsibilities

LEA shall provide system linkages, necessary Data extracts or permission access from LEA's student information or other systems on an agreed upon or pre-defined schedule between the Parties. Any such schedule agreed upon in writing (including by email) between the Parties shall be deemed incorporated herein and made a part hereof upon such mutual agreement.

3.1 Data extracts will be provided electronically by LEA to RCOE.

3.2 LEA will be responsible for providing the data needed to integrate LEA's Data into RCOE's data repositories as needed to perform the required tasks.

3.3 Data provided by LEA shall include Data relevant to the purpose of this MOU or specific system requirements.

3.4 LEA shall be responsible for determining which of their staff has access to system and communicating to RCOE the roles and responsibilities of each person with said access, including the person who is responsible for maintaining LEA's main and sub-accounts.

3.5 LEA shall designate those individuals who can: (a) transmit Data to RCOE; (b) request release of Data third parties; or (c) request extracts or analysis of LEA's Data.

### 4. Term

The term of this MOU shall be from **July 1, 2023** to **June 30, 2026**

### 5. Applicable Law

5.1 Data sharing under this MOU will from time to time include RCOE collecting and maintaining educational, personnel, medical and financial records that contain personally identifiable information (PII) on students or staff of LEA. RCOE is bound by the same regulations and laws as the LEA for access and management of this Data, and will conform to all legal requirements. RCOE and LEA agree that the disclosure of information under this MOU complies with the requirements of Education Code § 49073 et seq., FERPA, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), SOPIPA, and other state and federal/European Union laws and regulations regarding educational, personnel, medical and financial records.

5.2 The Parties understand that certain federal and state programs and laws, including the free and reduced lunch program and laws governing the provision of special education services, have additional legal requirements for data security, and both Parties agree to maintain full compliance with such requirements. Without limitation to the foregoing, RCOE and LEA additionally agree that aggregated (non-individually identifiable) and non-aggregated PII Data may be reported upon or shared as allowable by law.

5.3 RCOE and LEA shall ensure joint coordination and cooperation with one another to ensure compliance with FERPA, 20 U.S.C. § 1232g; 34 C.F.R. Part 99, as amended. The foregoing notwithstanding, RCOE and LEA agree that LEA shall be responsible for providing notices to parents required under FERPA,

obtaining necessary parental consent required under FERPA, and for providing parent(s), guardian(s) or student(s) with an opportunity to inspect and challenge the contents of Data shared with RCOE pursuant to this MOU.

## **6. Ownership of Data**

RCOE and LEA agree that LEA will continue to maintain ownership of and control over its source Data. RCOE agrees that it will not alter LEA's source Data without explicit authorization from LEA, and is not responsible for any errors therein. RCOE shall not be responsible for the type or quality of the Data provided by LEA, and RCOE makes no warranty as to the Data itself. LEA understands that though RCOE may notify it of issues it discovers with the source Data, LEA is responsible for any corrections required to its own Data or will authorize RCOE to make any limited explicit changes. LEA acknowledges that accurate reports rely upon accurate source Data being maintained by LEA. Each party owns or controls its data systems and the work product generated by such systems.

## **7. Prohibited Use of Data**

Except as otherwise permitted by the terms of this MOU, RCOE shall not use the Data supplied to it in an unauthorized manner. Specifically, RCOE shall not sell or release Data, nor enable or permit third parties to engage in targeted advertising to students or to build student profiles unrelated to the purposes intended by this MOU.

## **8. Student and Parent Access to Data**

When needed, RCOE shall work with LEA to provide a means by which employees, when authorized by LEA, can search and access student Data through reasonable procedures for LEA to respond to a parent, legal guardian, or eligible student who seeks to review PII in the pupil's records and to correct erroneous information. The foregoing notwithstanding, RCOE shall cooperate with LEA to help ensure this record correction will be consistent with LEA's policies regarding record correction.

## **9. Third-Party Vendors and Agencies**

Third parties may include but are not limited to public agencies the Parties desire to collaborate with, public agencies the Parties are required to share Data with, and/or any third-party vendor of either Party. Permission for RCOE to share Data with a third-party must be first granted by LEA in writing, including by email. RCOE may not distribute student or staff Data to any third-parties except as permitted by this MOU or subsequent written permission, unless required by law. RCOE shall ensure that approved third-parties adhere to this MOU. RCOE will help ensure that any subcontractor or sub-processor that it engages, to process, store, or access Data, has adequate technical security and organizational measures in place to keep Data secure and comply with this MOU. RCOE will require any third party vendors and subcontractors to comply with any applicable state and federal laws and regulations regarding educational records and data privacy, including but not limited to: Education Code §§ 49073.1, 49076, and 49076.5; FERPA; HIPAA; and SOPIPA. A disclosure list of third-party processors is available for viewing and public access at <https://www.rcoe.us/departments/administration-and-business-services/operational-support-services/contracts-and-purchasing/datasharing-memorandum-of-understanding-exhibit-a-vendor-list-827> .

9.1 RCOE may be required by subpoena or other lawfully issued order to divulge Data to law enforcement or another agency. When permitted by the requesting agency, RCOE shall provide LEA with notice of the request and types of information requested. Both RCOE and LEA have periodic needs to share Data, as legally allowed, with public agencies needing access to such Data to provide services to students. RCOE and LEA understand that sharing Data for use in such systems streamlines the process of providing services to

students. RCOE agrees that no Data will be made accessible to any such agency for any purpose other than those limited to the Data required and only under conditions allowed by law. Education Code §§ 49076 and 49076.5, as amended, and 20 U.S.C. § 1232g and 34 C.F.R. § 99.31, as amended, provide specific conditions under which Data may be accessed by or shared with public agencies.

9.2 RCOE may have periodic needs to share Data, as legally allowed, with university researchers for academic purposes to allow university researchers to collaborate with LEA and RCOE or to perform relevant research studies. RCOE shall notify LEA in writing, including by email, of any Data sharing pursuant to this Section, as follows:

1. Describe the identity of the researchers/organizations to whom the Data will be transmitted
2. Provide copies of contracts when requested, which shall include provisions binding the researcher/organization to the terms of this MOU
3. Describe the types of Data to be transmitted
4. Describe the manner in which the Data shall be de-identified or aggregated.

## 10. Independent Contractors for Data System Technical Support

Both Parties may engage the services of outside professionals in the course of administration, development or technical support of data systems. Any such professionals will be bound at all times by the same confidentiality and security requirements which are applicable to any Data within the Parties' systems, and by state and federal law governing such access.

## 11. Data Security

Both Parties agree to maintain appropriate security protocols in the transfer or transmission of Data, including ensuring Data may only be viewed or accessed by Parties legally allowed to do so. RCOE shall maintain Data obtained or generated pursuant to this MOU in a secure computer environment and not copy, reproduce, or transmit Data obtained pursuant to this MOU, except as allowed by LEA. RCOE shall provide security training to those of its employees who operate or have access to the system. RCOE may also provide an initial security training to LEA. RCOE shall provide LEA with contact information for the person at RCOE who LEA may contact if LEA has security concerns or questions. Where applicable, RCOE will require unique account identifiers, user names, and passwords that must be entered each time a client or user signs in. A description of RCOE's data security practices and procedures is attached to this MOU as Appendix A.

## 12. Data Breach Notification

RCOE shall maintain Information Security & Privacy Insurance with Electronic Media Liability policy with coverage limits of no less than one million dollars (\$1,000,000.00) per occurrence and five million dollars (\$5,000,000.00) aggregate for the duration of this MOU. Such policy shall cover damages resulting from the unauthorized access to, or theft of, data obtained by RCOE in connection to this MOU, as well as the unauthorized disclosure or use of (PII) that RCOE may acquire from LEA ("Data Breach"). It is further agreed and understood that the policy shall include coverage for crisis management costs, credit-monitoring expenses, payment of monies requested in connection to cyber extortion of LEA Data, and defense costs, fines, and penalties related to a Data Breach. Parties agree that the insurance requirements referred to herein shall apply to any third-party vendors hired by RCOE that may obtain or maintain LEA Data, as well as the outside agencies referred to in Section **Error! Reference source not found.** of this MOU. LEA reserves the right to request proof of insurance from RCOE, third-party vendors, and outside agencies to confirm compliance with these insurance requirements. Upon becoming aware of any unlawful or unauthorized access to student or staff Data stored on equipment used by RCOE or in facilities used by RCOE, RCOE will take the following measures:

12.1 Promptly file a claim with RCOE's Information Security & Privacy Insurance with Electronic Media Liability policy provider.

12.2 Promptly notify LEA of the suspected or actual incident, including the type of Data subject to unauthorized access.

12.3 Promptly investigate the incident and provide LEA with detailed information regarding the incident, including the identity of the affected users, and the estimated date of the breach.

12.4 Assist LEA in notifying either the student or their legal guardian, and take commercially reasonable steps to mitigate the effects and to minimize any damages resulting from the incident.

### **13. Indemnification and Liability**

Each Party agrees to indemnify the other against any and all liability, actions, claims, damages, losses, costs, and expenses (including attorneys' fees) arising out of or in any way resulting from the indemnifying Party's own negligent or intentional acts, errors, or omissions in connection to the performance of the responsibilities of each Party, per this MOU. The Parties shall not be held liable for any special, consequential, indirect or incidental damages incurred as a result of this MOU. The Parties shall be held harmless for any claims or lawsuits arising out of the release of information pursuant to a request by one of the Parties in conformity with this MOU or pursuant to law, excluding such release in connection to the negligence of either Party, or that of its officers, agents, or employees. If liability, damages, or any other claim relating to Data shared pursuant to this MOU is a result of a third party's act or omission, then the indemnification and defense that the third party contractually owes to RCOE and/or LEA shall also be extended to the other Party to this MOU, to the maximum extent possible.

### **14. Severability**

If any provision of this MOU is determined by a court to be invalid, unenforceable or otherwise ineffective, that provision shall be severed from the rest of this MOU, and the remaining provisions shall remain in effect and enforceable.

### **15. Modifications**

This MOU may be periodically or annually updated to incorporate changes if required upon mutual agreement of the Parties. Revisions required by changes to statute or notification of revisions to RCOE security policies will be issued by an amendment to this MOU as necessary. LEA understands that this MOU is part of an effort to standardize data sharing and management between RCOE and all districts it serves, and as such, every effort will be made to maintain a common agreement across all agencies.

### **16. Termination**

Either Party may terminate this MOU upon ninety (90) days' written notice. Upon termination or expiration of this MOU, RCOE shall work with LEA for the orderly cessation of extracts of student Data. Upon termination or expiration of this MOU, RCOE shall return or delete personally identifiable student Data unless otherwise provided by law or mutual agreement of the Parties. RCOE and LEA understand that RCOE may have an ongoing need to reference the raw Data it acquired during the term of this MOU. In the event that such need arises, RCOE shall, to the extent possible and subject to the mutual agreement of the LEA, only retain anonymized, aggregated Data that it obtained from LEA during the term of this MOU. However, RCOE certifies

that such anonymized, aggregated Data shall be purged when the Data has exceeded its useful life and shall not be kept for more than seven (7) years unless otherwise legally required.

**17. Dispute Resolution**

In the event of a dispute between any Party to this MOU, the parties shall attempt to resolve their disputes informally, in discussions involving the decision-makers for each of the parties. If these discussions are not successful, the parties shall retain a mediator to resolve the dispute with the mediation to be held within ninety (90) days of the date the dispute arises. If mediation is not successful, either party shall have the right to bring the dispute before the Riverside County Superior Court.

By signing this Agreement, CONTRACTOR acknowledges and agrees to the terms and conditions including the following exhibits:

- A. **APPENDIX A-RCOE Data Security Practices and Procedures**

**IN WITNESS WHEREOF**, the Parties agree to this Memorandum of Understanding to be executed by their duly authorized officers in the County of Riverside, State of California.

**Riverside County Superintendent of Schools**

**Perris Union High School District**

Signed \_\_\_\_\_  
Authorized Signature

Signed \_\_\_\_\_  
Authorized Signature

\_\_\_\_\_  
Printed Name and Title

\_\_\_\_\_  
Printed Name and Title

Date \_\_\_\_\_

Date \_\_\_\_\_

## Appendix A

### **RCOE Data Security Practices and Procedures**

Introduction: RCOE has established an Information Security (InfoSec) Program based on industry best practices and the needs of California K12 systems. The InfoSec program involves several departments, including Operational Support Services, Personnel Services, and Information Technology Services. The departments are primary functional units that will engage with legal counsel and security service/solution providers to develop and execute improvement plans. This plan may be periodically updated to take into account improving practices and technologies and to respond to a changing threat environment. LEAs will be provided with annual updates where there have been material modifications to the practices and procedures stated below.

As of July 20, 2018, the Program has identified the following areas to be part of the continual improvement of the RCOE InfoSec practices.

1. Anti-Virus/Malware Administration and Configuration
  - a. Regularly review and examine the policies and procedures related to Anti-virus/Malware controls and the configuration of Anti-virus/Malware software and appliances
  - b. Continual improvement of Anti-virus/Malware software configuration, operation and security
  - c. Provide Anti-virus/Malware training and awareness
  - d. Practice in depth Anti-virus/Malware defense for server and end user computers
  
2. Continuity of Operations Plan (COOP) and Disaster Recovery Plan (DRP)

COOP is the collection of sets of processes and procedures carried out by an organization to ensure that essential business functions continue to operate during and after a disaster. As part of the COOP there is a DRP. These are the technical plans developed for specific groups within an organization to allow them to recover a particular business application. RCOE addresses these plans by:

  - a. Performing annual Business Impact Analysis with various departments to identify mission critical processes and/or departments and prioritize the recovery processes and/or departments in accordance with their level of criticality
  - b. Secure Executive Oversight and Support for the COOP
  - c. Continual updates of documentation, content, sufficiency, testing and documentation of test results of the plans
  
3. Firewall Administration and Configuration
  - a. Examine and document the policies and procedures related to the administration of the organization's firewall(s)
  - b. Examine and document configuration files and access control lists for the devices and/or applications and operating systems
  - c. Implement least privilege access
  - d. Documentation, content and sufficiency of firewall policies and procedures
  - e. Logical placement of firewalls
  - f. Restricted access to management interfaces
  - g. Continual evaluation of applied rule sets
  - h. Backup, recovery, and storage of configuration files
  - i. Firewall event log review and sufficient storage for retention policy
  
4. Network Systems and Database Vulnerability Scanning

Perform scheduled simulations of attacks on the network and database systems by utilizing industry best of breed tools, which identify the vulnerabilities in the systems and provide recommendations for remediation.

5. Network Monitoring & Intrusion Detection
  - a. Regularly review the event logs to identify and correlate unauthorized, unusual, and sensitive access activity, such as:
    1. Attempted unauthorized logical and physical access;
    2. Access trends and deviations from those trends;
    3. Access to sensitive data and resources;
    4. Highly-sensitive privileged access, such as the ability to override security controls;
    5. Access modifications made by security personnel; and
    6. Unsuccessful attempts to logon to a system.
  - b. Improve documentation, content and sufficiency of network monitoring and intrusion detection policies and procedures
6. Patch Management
  - a. Regularly review and update systems, configuration, and applications for required systems
  - b. Sufficient testing of systems before and after patching
  - c. Maintain documentation of patch history of required systems
7. Physical Security

To prevent unauthorized personnel from gaining direct access to RCOE facilities that house sensitive information, the following areas are under a regular review and improvement process:

  - a. Documentation, content and sufficiency of physical security policies and procedures
  - b. External: facility perimeter, perimeter lighting, parking areas, parking area lighting, landscaping, exterior building lighting, exterior doors and locks and other entry points
  - c. Internal: doors, windows, ceilings, raised floors, wiring and utility closets, ceilings, attics, basements, crawlspaces and public areas
  - d. Lock and Key control
  - e. Access control including identification systems in use and access points
  - f. Intrusion alarms
  - g. Fire detection, suppression and prevention
  - h. CCTV/digital imaging technologies
  - i. Power system and utility control points
  - j. Documentation, retired network storage, and refuse disposal
  - k. Mail Handling
  - l. Hard copy record storage
  - m. Network Operations Center
8. Server (Data Center Systems) Administration and Configuration

Continual improvement of the following areas:

  - a. Documentation of server implementations, policies, and procedures
  - b. Hardware, operating system, and application security
  - c. User account policy and rights assignments
  - d. Auditing policies, system changes, user rights, and access to sensitive data
  - e. Event and security log retention and regular review
  - f. Critical file and folder permissions
  - g. Remote access and security
9. Network Switch and Router Administration and Configuration

Continual improvement of the following areas:

  - a. Develop clear documentation, content and sufficiency of policies and procedures
  - b. Streamline installation, operation and security



- c. Regular review of configuration
10. Workstation Administration and Configuration  
Continual improvement of the following:
- a. Documentation of workstation policies and procedures
  - b. Hardware security
  - c. Operating System installation, configuration and maintenance (patching)
  - d. User account policies and rights assignments
  - e. Event and security log settings and retention
  - f. Critical file and folder permissions
  - g. Remote access and security
11. Mobile Devices  
Regularly examine RCOE's policies and procedures related to administration of the mobile devices assigned to staff and students. The mobile devices include laptops, tablets and smartphones for both RCOE owned devices and personal devices brought onto RCOE's network.
12. Application Security Assessment and Mitigation  
The primary objective is to assess how effectively and efficiently RCOE ensures that no single trusted IT system user, administrator, or vendor is able to exploit vulnerabilities in RCOE's IT systems to accomplish and/or conceal an unauthorized diversion of RCOE's assets. Identify where the risk exists and evaluate the controls designed to mitigate this risk. Regularly review, evaluate, and update, if necessary, of the following IT controls:
- a. Database administration practices.
  - b. Production control practices.
13. Users Awareness Training  
Develop and update timely and relevant training material to raise the level of cybersecurity awareness of users throughout the organization.