Student Data-Sharing and Security Addendum

Rainey Day Rising Scholars Program | School and District Template

Document status	Pilot Template | July 2026
Prepared for	Rainey Day College Foundation, Inc. and participating school partners

IMPORTANT REVIEW NOTE. This is a customizable operational template, not legal advice. Each school or district should review it under applicable federal, state, local, procurement, and student-privacy requirements before signature or use.

This Addendum is incorporated into the School Partnership MOU or other underlying agreement between Rainey Day College Foundation, Inc. ("RDCF") and [SCHOOL / DISTRICT LEGAL NAME] ("School Partner"). If there is a conflict concerning student data, this Addendum controls unless applicable law requires otherwise.

1. Purpose and scope

This Addendum governs any approved disclosure, receipt, storage, use, access, transmission, return, or destruction of identifiable student information. It does not authorize a disclosure that is not otherwise permitted by law. The Parties will minimize data and use aggregate or properly de-identified information whenever it can accomplish the purpose.

2. Definitions

- Student Data: information directly related to an identifiable student that RDCF receives from or on behalf of the School Partner, including personally identifiable information from education records.
- Security Incident: unauthorized acquisition, access, use, disclosure, alteration, loss, destruction, or unavailability of Student Data, or a material compromise of systems that store or process it.
- Authorized User: an individual approved by RDCF whose access is necessary for the permitted purpose and who is bound by confidentiality and security duties.
- Subprocessor: a third party engaged by RDCF to store, transmit, or process Student Data.

3. Legal authority and documentation

Before each disclosure, the School Partner will document the legal basis it relies upon. In most community-organization referrals, the Parties expect to use signed and dated parent or eligible-student consent. If an exception to consent is proposed, the School Partner must identify and approve that exception in writing; neither this Addendum nor the MOU independently establishes that an exception applies.

4. Permitted purpose and use restrictions

- Use Student Data only for the purpose described in Exhibit A and only during the approved term.
- Do not sell, rent, monetize, advertise with, profile for unrelated purposes, or build unrelated products from Student Data.
- Do not redisclose Student Data except to an approved Subprocessor or as required by law after notice when legally permitted.
- Do not attempt to re-identify properly de-identified data or combine it with other information to identify a student.
- Do not make solely automated decisions that materially affect student eligibility or benefits without documented human review.
- Do not contact a student outside the approved family and school communication framework.

5. Data minimization and approved elements

RDCF may receive only the data elements listed in Exhibit A. Full rosters, complete transcripts, Social Security numbers, medical or disability information, detailed discipline records, financial-account information, immigration information, authentication credentials, and government identifiers are excluded unless separately approved in writing as necessary and lawful.

6. Access controls and workforce safeguards

- Restrict access by role and least privilege; review access at least quarterly and promptly remove access when duties end.
- Require unique accounts, strong passwords, and multi-factor authentication for administrative or staff access where supported.
- Maintain confidentiality commitments and annual privacy/security training for personnel with Student Data access.
- Log material administrative access and changes where technically feasible, and investigate suspicious activity.
- Prohibit downloading Student Data to unmanaged personal devices or sharing through personal accounts.

7. Technical and physical safeguards

- Encrypt Student Data in transit using current secure protocols and at rest where supported by the hosting service.
- Use supported software, timely security updates, malware protection where appropriate, secure configuration, backups, and vulnerability remediation proportionate to risk.
- Separate production access from public website access; do not expose Student Data through public pages or public search indexing.
- Maintain recovery procedures and test the ability to restore critical records.
- Protect paper records and physical media in locked, access-controlled locations and securely destroy them when no longer needed.

8. Secure transfer

The Parties will use the transfer method listed in Exhibit A. Ordinary unencrypted email, consumer text messaging, public links, and removable media without approved encryption are not authorized for Student Data. Each transfer should be limited to the minimum records needed and confirmed by the intended recipient.

9. Security incident response

RDCF will notify the School Partner's designated privacy/security contact without unreasonable delay and no later than [24/48] hours after confirming a Security Incident involving Student Data, unless law requires faster notice. Initial notice may be preliminary and will be supplemented as facts become available.

- Notice should describe the incident, discovery date, affected systems and data, known or estimated students affected, containment steps, remediation, and a response contact.
- RDCF will preserve relevant evidence, cooperate with reasonable investigation and legally required notices, and not notify families or the media on the School Partner's behalf unless coordinated or legally required.
- Responsibility for costs, notices, credit monitoring, or other remedies will be determined by applicable law and the final negotiated agreement.

10. Subprocessors

RDCF may use Subprocessors only when needed for the permitted purpose and only under written terms requiring privacy, security, incident response, use limitations, and return or destruction protections at least as protective as applicable portions of this Addendum. RDCF remains responsible for managing its Subprocessors. List approved Subprocessors in Exhibit A or an attached schedule.

11. Retention, return, and destruction

RDCF will retain Student Data only for the period listed in Exhibit A or as required by law. At expiration, termination, completion of purpose, or School Partner request, RDCF will return or securely destroy Student Data within [30/60] days unless retention is legally required. Any legally retained copy remains protected and may not be used for another purpose. On request, RDCF will provide written certification of destruction.

12. Student and family requests

The School Partner remains responsible for responding to FERPA access, amendment, complaint, and records requests concerning its education records. RDCF will reasonably assist by locating, exporting, correcting, or deleting relevant Student Data when directed and legally appropriate. RDCF will refer direct education-record requests to the School Partner unless the Parties agree otherwise.

13. Records, oversight, and verification

- Maintain a current inventory of systems, approved users, subprocessors, and data categories used for the program.
- Provide reasonable written information necessary for the School Partner's privacy, security, procurement, and compliance review.
- Upon reasonable notice, cooperate with a proportionate review of compliance that protects RDCF security information and other clients' confidentiality.
- Promptly remediate material deficiencies identified by either Party.

14. Compelled disclosure

If legally compelled to disclose Student Data, the receiving Party will, when legally permitted, provide prompt notice to the other Party, disclose only what is legally required, and seek appropriate protective treatment.

15. Term, survival, and order of precedence

This Addendum begins on [DATE] and continues while RDCF possesses Student Data. Use restrictions, confidentiality, security incident cooperation, return/destruction, and other provisions intended by their nature to survive will continue after termination. Final district-approved terms regarding insurance, indemnification, limitation of liability, venue, public records, and governing law should be inserted or incorporated here: [DISTRICT TERMS / REFERENCE].

Exhibit A - Approved data and operating schedule

Program purpose	Eligibility verification, consent-based referral, college-readiness support, approved evaluation
Student population	[GRADES / SCHOOLS / ESTIMATED COUNT]
Legal basis	[SIGNED CONSENT / SPECIFIC APPROVED EXCEPTION AND CITATION]
Approved data elements	[LIST EACH FIELD; DO NOT WRITE “ALL STUDENT DATA”]
Excluded data	SSN, financial accounts, credentials, detailed medical/disability/discipline/immigration data unless separately approved
Source and recipient	[SCHOOL ROLE / SYSTEM] to [RDCF ROLE / SYSTEM]
Transfer method	[APPROVED SECURE PORTAL / ENCRYPTED TRANSFER]
Update frequency	[ONE-TIME / TERM / EVENT-BASED]
Retention period	[PERIOD / EVENT], followed by return or destruction within [30/60] days
Approved subprocessors	[PROVIDER, SERVICE, DATA, HOSTING REGION, CONTRACT DATE]
School privacy/security contact	[NAME, ROLE, EMAIL, PHONE]
RDCF privacy/security contact	[NAME, ROLE, EMAIL, PHONE]

Exhibit B - Security review checklist

[ ] Staff access is role-based and limited to approved users.

[ ] Multi-factor authentication is enabled for staff/administrative access where supported.

[ ] Encryption in transit and at rest is documented.

[ ] Backups and recovery procedures are documented and tested.

[ ] Security updates and vulnerability remediation responsibilities are assigned.

[ ] Incident-response contacts and notification timelines are confirmed.

[ ] Subprocessors and their access are documented and contractually restricted.

[ ] Retention and secure destruction are configured and assigned.

[ ] Public website routes cannot retrieve or expose student records.

[ ] Annual privacy/security training and confidentiality obligations are documented.

Exhibit C - Incident and destruction records

Incident notification address	_____
After-hours security contact	_____
Initial notice deadline	_____
Family notification decision-maker	_____
Records return date	_____
Records destruction date	_____
Certification provided by / date	_____

Signatures

RAINEY DAY COLLEGE FOUNDATION, INC.	
Authorized representative	_____
Title	_____
Signature	_____
Date	_____
Email / phone	_____
[SCHOOL / DISTRICT LEGAL NAME]	
Authorized representative	_____
Title	_____
Signature	_____
Date	_____
Email / phone	_____

Reference framework

Drafting references (accessed July 2026):

- U.S. Department of Education, FERPA and Volunteer and Partnership Organizations: https://studentprivacy.ed.gov/sites/default/files/resource_document/file/ferpa-and-community-based-orgs_2021.pdf
- U.S. Department of Education, FERPA regulations and guidance: https://studentprivacy.ed.gov/ferpa
- U.S. Department of Education, Privacy and Data Sharing resources: https://studentprivacy.ed.gov/privacy-and-data-sharing
- U.S. Department of Education, Directory Information guidance: https://studentprivacy.ed.gov/content/directory-information