SCHOOL DATA ADDENDUM

FERPA / COPPA / State Student-Privacy Compliance Addendum

between

Jal Technology LLC d/b/a QRCodeKey

647 Rose Lane, Bartlett, Illinois 60103, USA

and

[SCHOOL / DISTRICT / INSTITUTION LEGAL NAME]

[School address line 1]

[School address line 2]

Effective Date: _____

Template Version 1.0 — May 2026

Recitals

This School Data Addendum (this "Addendum") is entered into as of the Effective Date by and between Jal Technology LLC, an Illinois limited liability company doing business as QRCodeKey ("QRCodeKey", "Service Provider", or "Company"), and the school, school district, college, university, or other educational institution identified on the cover page (the "School"). QRCodeKey and the School are referred to individually as a "Party" and collectively as the "Parties".

WHEREAS, the School is an "educational agency or institution" as that term is used in the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, and the implementing regulations at 34 C.F.R. Part 99 ("FERPA"), or is otherwise subject to one or more state, federal, or foreign student-privacy laws;

WHEREAS, the School has subscribed to one or more services of QRCodeKey (the "Services") under the QRCodeKey Terms of Service available at qrcodekey.com/terms (the "Underlying Agreement"), and may, in the course of using the Services, share or cause to be shared certain "education records" or other student personal information with QRCodeKey;

WHEREAS, the Parties wish to ensure that any such sharing complies with FERPA, COPPA, and applicable state student-privacy laws, including without limitation the California Student Online Personal Information Protection Act (Cal. Bus. & Prof. Code §§ 22584-22585) ("SOPIPA"), New York Education Law § 2-d, the Illinois Student Online Personal Protection Act (105 ILCS 85) ("SOPPA"), the Connecticut Student Data Privacy Act (Public Act 16-189), the Colorado Student Data Transparency and Security Act (HB 16-1423), the Maryland Student Data Privacy Act, the Texas Education Code § 32.151 et seq., and analogous laws in other US states and other jurisdictions (collectively, "Student-Privacy Laws");

NOW, THEREFORE, in consideration of the mutual covenants and agreements set forth in this Addendum, the Parties agree as follows.

1. Definitions

“Education Record” means "education records" as defined in 20 U.S.C. § 1232g(a)(4) and 34 C.F.R. § 99.3 — records, files, documents, and other materials that contain information directly related to a student and are maintained by the School or by a party acting for the School.

“Personally Identifiable Information (“PII”)” means "personally identifiable information" as defined in 34 C.F.R. § 99.3, including the student's name, the name of the student's parent(s) or family member(s), the student's address, a personal identifier (such as student ID number or biometric record), other indirect identifiers, and any other information that, alone or in combination, would allow a reasonable person in the school community to identify the student.

“Student Data” means collectively, Education Records, PII, and any other information about a student, parent, or guardian that is provided to or accessed through QRCodeKey by or on behalf of the School.

“School Official” means a "school official" with a "legitimate educational interest" as those terms are used in 34 C.F.R. § 99.31(a)(1)(i)(B), to whom the School may disclose Education Records without prior written parental consent.

“Targeted Advertising” means presenting an advertisement to a student where the advertisement is selected based on Student Data obtained or inferred over time from a student's online behavior, usage of applications, or activities. The term does not include advertising selected on the basis of contextual information not derived from Student Data.

“Minor” means a student who is under the age of 18 (or, in the United States, under the age of 13 for purposes of the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506 ("COPPA"); or below the applicable age of digital consent in any other jurisdiction whose law applies).

2. School Official Designation; Direct Control

2.1 Designation

The School designates QRCodeKey as a "School Official" under 34 C.F.R. § 99.31(a)(1)(i)(B) and acknowledges that QRCodeKey performs an institutional service or function for which the School would otherwise use its own employees. The School determines that QRCodeKey has a "legitimate educational interest" in Student Data only to the extent reasonably necessary to provide the Services.

2.2 Direct Control

QRCodeKey is, and shall remain, under the direct control of the School with respect to its use and maintenance of Education Records, as required by 34 C.F.R. § 99.31(a)(1)(i)(B)(2). QRCodeKey shall: (a) use Education Records only for the purposes for which the School has authorized, as set forth in this Addendum and the Underlying Agreement; (b) be subject to the requirements governing the use and re-disclosure of personally identifiable information from Education Records under 34 C.F.R. § 99.33(a); and (c) not re-disclose Student Data to any third party except as expressly permitted by this Addendum.

2.3 Ownership

All Student Data, including Education Records, is, and shall remain, the property of the School and the student or parent / legal guardian (as applicable). Nothing in the Underlying Agreement or this Addendum shall transfer ownership of Student Data to QRCodeKey. QRCodeKey acknowledges that it acquires no rights in Student Data other than the limited license to process the data for the purposes described in Section 3.

3. Permitted Uses of Student Data

3.1 Authorized Purposes

QRCodeKey may use Student Data only to: (a) provide the Services to the School; (b) maintain, support, evaluate, and improve the Services for the benefit of School customers, provided that any such improvement use does not result in the disclosure of Student Data; (c) respond to support requests from the School or its authorized users; (d) comply with applicable law; and (e) enforce the Underlying Agreement and this Addendum.

3.2 Prohibited Uses

QRCodeKey shall not, and shall not permit any third party to:

- Use Student Data for any commercial purpose other than providing the Services to the School;
- Engage in Targeted Advertising directed at any student, parent, or legal guardian using Student Data, regardless of whether the advertising appears within the Services or elsewhere;
- Sell, lease, trade, or otherwise transfer Student Data to any third party for monetary or other valuable consideration, except as part of a corporate transaction (merger, acquisition, sale of assets) where the successor entity is bound by terms substantially similar to this Addendum;
- Build a non-educational personal profile of a student, parent, or legal guardian (other than in furtherance of an authorized purpose under Section 3.1);
- Use Student Data to train any third-party machine-learning model;
- Use Student Data to amplify or recommend behavioral content to the student outside the educational context.

4. Parental and Guardian Consent for Minors

4.1 School Responsibility for Consent

The School represents and warrants that it has obtained, or shall obtain prior to onboarding any Student Data, all consents, authorizations, and notices required by FERPA, COPPA (for students under 13), state Student-Privacy Laws, and any analogous foreign law (including but not limited to GDPR Article 8, UK GDPR / DPA 2018, India DPDP Act 2023 Section 9, Brazil LGPD Article 14, China PIPL Article 31, Canada PIPEDA, Quebec Law 25, Australia Privacy Act 1988, Mexico LFPDPPP, and the local age-of-digital-consent in any other jurisdiction whose law applies). The School acknowledges that obtaining and documenting verifiable parental or legal-guardian consent is the School's sole responsibility, and that QRCodeKey is not the data controller for the Minor's Student Data.

4.2 Verifiable Methods

To the extent COPPA applies to a student under 13, the School shall obtain verifiable parental consent that meets the standard set forth in 16 C.F.R. § 312.5(b), and shall maintain a record of

the consent for as long as the Student Data is retained. To the extent GDPR Article 8, DPDP Section 9, or analogous laws apply, the School shall obtain consent through methods reasonably calculated to ensure that the person providing consent is in fact the parent or legal guardian of the Minor.

4.3 Withdrawal of Consent

Upon receipt of a request from a parent, legal guardian, or eligible student to withdraw consent or to delete the Minor's Student Data, the School shall (a) confirm the request in writing within ten (10) business days; and (b) instruct QRCodeKey through the QRCodeKey support channel to delete the Minor's Student Data, which QRCodeKey shall do within thirty (30) days of the School's instruction.

5. Security and Confidentiality

5.1 Safeguards

QRCodeKey shall implement and maintain administrative, technical, and physical safeguards designed to protect the security, confidentiality, and integrity of Student Data, including:

- Encryption of Student Data at rest using AES-256 (or stronger) and in transit using TLS 1.2 (or stronger);
- Role-based access controls, multi-factor authentication for administrative accounts, and audit logging of all Student Data access;
- Annual risk assessment, written information security policy, incident response plan, and business continuity / disaster recovery plan;
- Regular security training for QRCodeKey workforce members with access to Student Data;
- Background checks for all QRCodeKey workforce members with administrative access to Student Data, where permitted by law.

5.2 Sub-Processors

QRCodeKey may engage sub-processors to assist with the provision of the Services only if the sub-processor is bound by a written agreement that imposes obligations on Student Data handling that are at least as protective as this Addendum. QRCodeKey shall maintain a current list of sub-processors at qrcodekey.com/sub-processors and shall provide the School with notice of any new sub-processor that will handle Student Data at least thirty (30) days in advance, giving the School an opportunity to object.

6. Data Breach Notification

In the event of any unauthorized acquisition, access, use, or disclosure of Student Data (a "Data Breach"), QRCodeKey shall notify the School in writing without unreasonable delay and in any event no later than forty-eight (48) hours after QRCodeKey becomes aware of the Data Breach. The notice shall include, to the extent known: (a) the nature and scope of the Data Breach; (b) the categories and approximate number of students affected; (c) the categories and

approximate volume of Student Data records affected; (d) the steps QRCodeKey is taking to investigate, mitigate, and prevent recurrence; and (e) a contact at QRCodeKey for follow-up. QRCodeKey shall cooperate with the School's reasonable requests for information and assistance in connection with the School's notification obligations to parents, students, regulators (including state education agencies, the U.S. Department of Education, and applicable data-protection authorities), and the public.

7. Access, Amendment, and Deletion of Student Data

7.1 School Access

Upon written request from the School, QRCodeKey shall provide the School with reasonable access to Student Data in a portable, machine-readable format, at no additional charge, within fifteen (15) business days.

7.2 Parent / Eligible-Student Rights

QRCodeKey shall promptly forward to the School any request received directly from a parent, legal guardian, or eligible student to access, correct, or delete the student's Student Data, and shall not respond to such requests except at the direction of the School. The School shall be responsible for handling parent and eligible-student rights requests in accordance with FERPA and applicable Student-Privacy Laws.

7.3 Deletion

Upon termination of the Underlying Agreement, expiration of this Addendum, or written request from the School at any time, QRCodeKey shall delete all Student Data within sixty (60) days, except (a) backup copies that shall be deleted in accordance with QRCodeKey's ordinary backup retention cycle (not to exceed ninety (90) days); and (b) anonymized or de-identified data that no longer qualifies as Student Data under FERPA. QRCodeKey shall provide the School with a written certification of deletion upon request.

8. State-Specific Provisions

To the extent the School is subject to any of the following state Student-Privacy Laws, the corresponding provisions are incorporated into this Addendum and shall control over any conflicting provision:

- California — SOPIPA: QRCodeKey shall not use Student Data for Targeted Advertising, build a non-educational profile, or sell Student Data; deletion within statutory timeframe upon School request.
- New York — Education Law § 2-d: QRCodeKey shall comply with the Education Department's Parents' Bill of Rights for Data Privacy and Security; data shall not be sold or used for marketing.

- Illinois — SOPPA (105 ILCS 85): QRCodeKey shall publish on its website a list of categories of Student Data it collects, the purposes of collection, and any sub-processor; the School shall publish a list of operators with which it has signed agreements.
- Connecticut — Public Act 16-189: QRCodeKey shall not collect, use, or share Student Data beyond what is necessary for educational purposes authorized by the School.
- Colorado — HB 16-1423: QRCodeKey shall provide a clear and conspicuous notice on its website regarding its collection, use, and disclosure of Student Data.
- Maryland — Student Data Privacy Act: QRCodeKey shall not engage in Targeted Advertising; sub-processor disclosures and security obligations apply.
- Texas — Education Code § 32.151 et seq.: parental access, no Targeted Advertising, deletion on request, and breach-notification obligations apply.
- Other states: where the School is subject to a state Student-Privacy Law not listed above, the more protective standard between this Addendum and that law shall apply.

9. Term, Termination, and Survival

9.1 Term

This Addendum shall commence on the Effective Date and shall continue in effect for so long as the Underlying Agreement is in effect or QRCodeKey holds any Student Data, whichever is later.

9.2 Termination for Material Breach

Either Party may terminate this Addendum and the Underlying Agreement upon thirty (30) days' written notice if the other Party materially breaches this Addendum and fails to cure the breach within the thirty-day period.

9.3 Survival

Sections 5, 6, 7.3, 9, and 10 shall survive the termination of this Addendum.

10. Miscellaneous

10.1 Order of Precedence

In the event of a conflict between this Addendum and the Underlying Agreement with respect to Student Data, this Addendum shall control. With respect to all other matters, the Underlying Agreement shall control.

10.2 Assignment

Neither Party may assign this Addendum without the prior written consent of the other Party, except that QRCodeKey may assign this Addendum, without consent, in connection with a merger, acquisition, or sale of substantially all of its assets, provided that the successor entity is bound by the terms of this Addendum.

10.3 Indemnification

Each Party shall indemnify, defend, and hold harmless the other Party and its officers, directors, employees, agents, and successors from and against any third-party claims, demands, actions, suits, judgments, fines, penalties, losses, damages, settlements, costs, and expenses (including reasonable attorneys' fees) to the extent arising out of or resulting from the indemnifying Party's breach of this Addendum, negligence, or willful misconduct. The School specifically indemnifies QRCodeKey against claims arising from the School's failure to obtain or document parental or legal-guardian consent for any Minor under Section 4.

10.4 Limitation of Liability

Except for the indemnification obligations in Section 10.3 and either Party's breach of confidentiality obligations under Sections 3 and 5, neither Party's aggregate liability under or in connection with this Addendum shall exceed the limitation of liability set forth in the Underlying Agreement.

10.5 Governing Law and Venue

This Addendum is governed by, and shall be construed in accordance with, the laws of the State of Illinois (without regard to conflict-of-laws principles), except that mandatory provisions of FERPA, COPPA, and the State of the School's domicile shall apply where required by law.

10.6 Notices

Notices to QRCodeKey shall be sent to info.qrcodekey@gmail.com with a copy to the address on the cover page. Notices to the School shall be sent to the address and email on the cover page.

10.7 Counterparts; Electronic Signature

This Addendum may be executed in counterparts, each of which shall be deemed an original and all of which together shall constitute one and the same agreement. Electronic signatures shall have the same legal effect as original signatures.

10.8 Entire Agreement

This Addendum, together with the Underlying Agreement, constitutes the entire agreement between the Parties with respect to Student Data and supersedes all prior agreements.

Signatures

IN WITNESS WHEREOF, the Parties have caused this School Data Addendum to be executed by their duly authorized representatives as of the Effective Date.

SERVICE PROVIDER — Jal Technology LLC d/b/a QRCodeKey

By: _____

Name: Ashvinkumar Chaudhari

Title: Founder & Authorized Signatory

Date: _____

Email: info.qrcodekey@gmail.com

SCHOOL — [SCHOOL / DISTRICT / INSTITUTION LEGAL NAME]

By: _____

Name: _____

Title: _____

Date: _____

Email: _____

Appendix A — Categories of Student Data Collected

In the ordinary course of providing the Services, QRCodeKey may collect or process the following categories of Student Data on behalf of the School:

- Identifiers — student name, student ID number (if entered by School), email address, phone number, and date of birth (if entered).
- Attendance / scan data — timestamp of each QR scan, GPS location at the time of scan, device fingerprint, IP address.
- Group membership — which Group(s) the student is a member of within the School's QRCodeKey account.
- Visitor records (where the student is logged as a visitor) — name, photo (only if uploaded by the visitor at sign-in), signature, purpose of visit, sign-in / sign-out times.

QRCodeKey does NOT collect: biometric identifiers (face, voice, fingerprint, retina); academic grades, transcripts, or other curriculum-content data; disciplinary records; medical or special-education records.

Appendix B — Sub-Processor List

QRCodeKey uses the following sub-processors to provide the Services. Each sub-processor is bound by a written agreement that satisfies the requirements of this Addendum:

- MongoDB Atlas (database hosting; AES-256 at rest; SOC 2 Type II) — operated by MongoDB, Inc., New York, NY, USA.
- Render, Inc. (application hosting; SOC 2 Type II) — operated by Render Services, Inc., San Francisco, CA, USA.
- Vercel Inc. (frontend hosting; SOC 2 Type II) — operated by Vercel Inc., San Francisco, CA, USA.
- Stripe, Inc. (payment processing for paid School subscriptions; PCI-DSS Level 1) — operated by Stripe, Inc., San Francisco, CA, USA.
- Twilio Inc. / Telnyx LLC (SMS notification; A2P 10DLC brand-verified).
- OpenAI, L.L.C. (AI chatbot and voice agent; data-processing terms in effect; Student Data is NOT used to train OpenAI models).

The current list is also published at qrcodekey.com/sub-processors and is updated as sub-processors are added, replaced, or removed. The School will receive thirty (30) days' advance notice of any new sub-processor that will handle Student Data.

Appendix C — Parents' Bill of Rights for Data Privacy and Security (per New York Education Law § 2-d)

Where the School is subject to New York Education Law § 2-d, this Appendix C, together with the body of this Addendum, satisfies the Parents' Bill of Rights requirement:

- A student's Student Data cannot be sold or released for any commercial or marketing purpose.
- Parents have the right to inspect and review the complete contents of the student's education record.
- State and federal laws protect the confidentiality of Student Data; safeguards include encryption, firewalls, password protection, and access controls.
- A complete list of student data elements collected by the State is publicly available at the New York State Education Department website.
- Parents have the right to have complaints about possible breaches of student data addressed; complaints should be directed to the School and may be escalated to the New York State Education Department's Chief Privacy Officer.