

ARCHITECTURE OF GRACE

Student Data Privacy Agreement

Template, modelled on the SDPC National Data Privacy Agreement structure.

DISCLAIMER This is a **draft template for discussion**. It is not legal advice, and Architecture of Grace is not a law firm. It must be reviewed and customised by qualified counsel for the specific LEA and jurisdiction before execution. **Where an LEA participates in the Student Data Privacy Consortium, the LEA's own SDPC template for its state or alliance should be used instead**, with the exhibits here supplying the technical detail. Everything in square brackets is a field for the LEA to complete.

Version 2.0, 6 September 2026. Written against sync script version 11 (5 September 2026). Supersedes the June 2026 template, whose Exhibits described a single instrument, one shared passcode and four data elements. It should be read with the **Data & Privacy Statement v2.0** and the **IT Deployment & Data Guide v2.0**, which are incorporated by reference as Annexes 1 and 2.

Parties and term

This Student Data Privacy Agreement ("Agreement") is entered into by **[Local Education Agency / District Name]** ("LEA"), of **[LEA address]**, and **Architecture of Grace** ("Provider"), of **[Provider address]**. It is effective as of **[Effective Date]** and governs the LEA's use of the services described in Exhibit A.

Provider contact for privacy matters: **James Anthony Ramsden, Architecture of Grace — Theopus77@yahoo.com**. **[Update on execution if the Provider's contact address changes.]**

Recitals

WHEREAS the LEA wishes to use some or all of the Provider's services, which comprise **three separable layers** — a curriculum, a set of academic practice activities, and an optional check-in layer — as set out in Exhibit A; and

WHEREAS the parties intend to protect Student Data consistent with the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA) where applicable, the Protection of Pupil Rights Amendment (PPRA), the Individuals with Disabilities Education Act (IDEA) where the services touch a student with a disability, and applicable state law; and

WHEREAS the parties wish to define their obligations regarding the collection, use, protection and disposition of Student Data;

NOW, THEREFORE, the parties agree as follows.

Article I — Purpose and scope

1.1 This Agreement applies to all Student Data the Provider receives, accesses or stores in connection with the services described in Exhibit A.

1.2 The Provider shall use Student Data solely to provide the services to the LEA, and for no other purpose.

1.3 **The layers are separable, and the LEA may adopt fewer than all of them.** The curriculum layer collects nothing. The academic practice layer produces a practice record only where a student sends one. Only the

check-in layer asks a student about their own state. **An LEA that adopts only the curriculum creates no Student Data through these services at all**, and the obligations below attach to whichever layers the LEA in fact enables, as recorded in Exhibit A.

1.4 The optional public “Voices” comment wall is not Student Data and is not governed by this Agreement as a protected education record. Posts are public by design. Its governance is addressed in Exhibit B.

Article II — Definitions

2.1 “**Student Data**” means any information directly related to an identifiable student collected or maintained through the services, in any form, including a pseudonymous code where the LEA holds the key that links it to a named student.

2.2 “**De-Identified Data**” means data from which all direct and indirect identifiers have been removed such that a student cannot reasonably be identified.

2.3 “**Data Controller**” means the LEA, which owns and directs the use of Student Data. “**Data Processor**” means the Provider, acting only on the LEA’s documented instructions.

2.4 “**Destination**” means the system the LEA designates to receive synced records — ordinarily a Google Sheet in the LEA’s own Google Workspace tenant, reached through Google Apps Script.

2.5 “**Check-in layer**” means the instruments listed in Exhibit A, Part 3.

Article III — Data ownership, and the destination requirement

3.1 All Student Data is and remains the property of the LEA. The Provider obtains no ownership rights and acts solely as a Data Processor.

3.2 The LEA retains full control of configuration: whether records remain on the device or are transmitted; the Destination; which layers are enabled; and whether the Voices wall is on. The Provider shall not alter these without the LEA’s prior written consent.

THE DESTINATION MUST BE LEA-OWNED 3.3 The FERPA school-official exception requires the educational agency’s **direct control** of the data (34 CFR § 99.31(a)(1)(i)(B)(2)). Accordingly **the Destination shall be owned by the LEA**, on an institutional account under its own access, retention and audit policy. **A Destination hosted on an individual educator’s personal account does not satisfy this requirement and shall not be used for Student Data**, notwithstanding any convenience, pilot arrangement or prior practice.

3.4 The Provider operates no back-end for LEA deployments and does not retain synced Student Data after transmission to the Destination. Where the Provider incidentally receives Student Data — for example in a support request — Article VII applies to it.

Article IV — Permitted use; no sale, advertising, or AI training

4.1 The Provider shall not sell, rent, lease or trade Student Data.

4.2 The Provider shall not use Student Data for targeted advertising, to build a commercial profile of a student, or for any purpose beyond providing the services.

4.3 Any use of De-Identified Data for product improvement shall be limited to data that cannot reasonably identify a student, and shall never be re-identified.

4.4 Artificial intelligence. The Provider shall not use Student Data, whether identifiable or De-Identified, to develop, train, improve or fine-tune any artificial-intelligence, machine-learning or large-language model, and shall not disclose Student Data to any third party for that purpose. The Provider represents that no Student Data has been or will be used for such purposes.

Article V — Consent to administer the check-in layer

5.1 Enabling sync is a data decision. **Administering the check-in layer is a consent decision, and they are separate.** This Article addresses the second.

5.2 The LEA shall obtain **written parental consent in advance, with the questions attached**, before administering any instrument in the check-in layer, unless the LEA's counsel determines on the record that a different basis applies in its jurisdiction. The Provider supplies a ready-to-adapt consent packet in English and Spanish, with all nineteen statements attached rather than summarised.

5.3 The Provider's position follows the U.S. Department of Education Student Privacy Policy Office's Dear Colleague Letter of 26 August 2026, which takes the view that a survey touching a student's emotional or psychological state is "required" once a school official administers it, that this does not depend on federal funding, and that PPRA's opt-out provisions do not secure consent for such a survey.

STATED AS CONTESTED That letter is sub-regulatory guidance issued without notice and comment, and a broadly similar letter was set aside in litigation in 2025. The Provider follows it because the two errors are not symmetrical: consent under a reading later held too broad costs paperwork, while an opt-out under a reading that holds costs a school year on an instrument that touched every student. **The LEA should reach its own conclusion with its own counsel, and record it.**

5.4 The curriculum and academic practice layers are not surveys and are not subject to this Article. The LEA retains PPRA's instructional-materials inspection rights in respect of them.

5.5 The LEA shall not describe or record the curriculum and the check-in layer as a single undifferentiated programme, since doing so forfeits the distinction this Article and Article I.3 rest on.

Article VI — Limits on use for students with disabilities

6.1 The check-in layer is **not a validated instrument** and is not diagnostic. It produces flags for a supportive conversation.

6.2 The LEA shall not use output from the check-in layer as the sole basis for determining whether a student is a child with a disability, or for determining an appropriate educational programme or the content of an IEP (see 34 CFR §§ 300.304(b)(1)(ii) and (b)(2)).

6.3 Where the LEA relies on 34 CFR § 300.302 — screening by a teacher or specialist to determine instructional strategies — it acknowledges that the exemption is **purpose-bound**, and is lost where the instrument is run on a single suspected child, read for eligibility, read to determine IEP content, or read to judge whether an existing IEP's supports are working.

6.4 Section 504 requires validated instruments for evaluation purposes (34 CFR § 104.35(b)(1)). The check-in layer does not meet that standard and shall not function as evaluation material.

6.5 Notes entered by staff within the services shall not be characterised as sole-possession records. Once a note is synced, printed into a meeting document, or incorporated into a chart, it has been disclosed and is an education record.

Article VII — Security, and its stated limits

7.1 The Provider shall maintain administrative and technical safeguards appropriate to the sensitivity of the data. Records are transmitted over TLS to the Destination the LEA designates.

7.2 Implemented controls (script version 11, 5 September 2026): every string written to the Destination is escaped so that a submitted value cannot become a live spreadsheet formula; request bodies over 65,536 bytes are rejected before parsing and any single field over 2,000 characters is truncated; each key is limited to 300 requests per minute; unrecognised request types are rejected and write nothing; and every write path appends exactly one row. Reading occurs only over POST — no credential travels in a URL or browser history.

7.3 Two keys. Writing and reading use separate secrets held in the LEA's own Apps Script project properties. The write key is published in the site's configuration file and is public by design; the read key is never published.

KNOWN LIMITATIONS — DISCLOSED, NOT WARRANTED AWAY The LEA acknowledges, and the Provider affirmatively discloses, that: **(a)** the public write key allows anyone who reads it to append rows carrying real student identifiers, invented scores and safety flags, attributed to a named staff member, and such forged rows are not distinguishable from genuine ones; it cannot read, alter or delete; **(b)** the read key is **not scoped** — a holder receives every row in that Destination, across all students, classes and staff; **(c)** the services provide **no per-user authentication**, and the results view is gated by a convenience code that performs no encryption. **Compensating controls are set out in Exhibit C and are the LEA's to operate.**

7.4 The Provider shall not access Student Data except as necessary to provide support the LEA has requested, and shall record any such access.

Article VIII — Breach and incident response

8.1 The Provider shall notify the LEA without unreasonable delay and in any event within **seventy-two (72) hours** of discovering unauthorised access to, acquisition of, or disclosure of Student Data — or within any **shorter period required by applicable state law**, whichever is earlier. **[Illinois: see the SOPPA addendum at Exhibit E.]**

8.2 The notice shall describe, so far as known: the nature of the incident; the categories and approximate number of individuals affected; the types of Student Data involved; and the steps taken or planned to mitigate harm. The parties shall cooperate on any required notifications.

8.3 Where an incident arises within the LEA's own Destination — for example through misuse of the read key, or sharing of the Destination beyond those with a legitimate educational interest — the LEA is the controller of that system and leads the response, with the Provider's reasonable assistance.

Article IX — Retention, return and destruction

9.1 Retention of records in the Destination is set and operated by the LEA, **not by the Provider and not by the software**. The LEA shall configure a retention period that satisfies its own law.

RETENTION CANNOT BE A PRODUCT CONSTANT State requirements pull in opposite directions. Illinois treats this as a temporary student record with a **five-year minimum** and ten business days to produce on request (105 ILCS 10). Louisiana requires **destruction within thirty days**. The LEA's period: [_____], reviewed [annually / other].

9.2 On the LEA's written request or on termination, the Provider shall within **thirty (30) days** securely return or destroy any Student Data in its possession or control and certify destruction in writing. In the ordinary LEA-owned configuration the Provider holds none.

9.3 Records held only in a browser on an end-user device are removed by clearing that browser's storage, or through the deletion control in the results view. The Provider has no ability to reach them.

Article X — Subprocessors

10.1 The Provider shall maintain a current list of subprocessors and provide it on request. As configured, the data path involves: **Google LLC**, as the operator of the LEA's own Workspace tenant, Apps Script and Sheets — engaged under the LEA's own agreement with Google, not the Provider's; the LEA's or Provider's **static web host**, which serves files and receives no Student Data; and **Google Fonts**, which receives ordinary technical request information and never any response content.

10.2 Any subprocessor shall be bound by obligations no less protective than these. The Provider remains responsible for its subprocessors.

Article XI — Parent and student rights

11.1 The LEA retains sole responsibility for responding to requests to access, correct, amend or delete Student Data. The Provider shall assist within a commercially reasonable time. Where the Destination is LEA-owned, the LEA can satisfy such a request directly and without the Provider.

11.2 The LEA shall make the questions in the check-in layer available for inspection on request, and the Provider shall keep a current copy of all nineteen statements published for that purpose.

Article XII — Term, termination and miscellaneous

12.1 This Agreement continues for the duration of the services relationship and survives as to confidentiality, data disposition and any obligation that by its nature should survive.

12.2 Either party may terminate on thirty (30) days' written notice. Article IX then applies.

12.3 Governing law. The laws of the State of [State], without regard to conflict of laws.

12.4 General offer. The Provider may extend these terms to other LEAs that countersign Exhibit F, consistent with the SDPC general-offer model, subject to each LEA's independent review.

12.5 Entire agreement. This Agreement with its Exhibits is the entire agreement and may be amended only in writing signed by both parties. **If any provision conflicts with the LEA's required SDPC template or mandatory district policy, the LEA's template or policy controls.**

12.6 Limitation of liability. TO THE MAXIMUM EXTENT PERMITTED BY LAW, NEITHER PARTY SHALL BE LIABLE FOR INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES. THE PROVIDER'S TOTAL LIABILITY SHALL NOT EXCEED [the greater of the fees paid in the preceding twelve months, or \$_____].

12.7 Severability. If any provision is held invalid, the remainder continues in force.

Signatures

IN WITNESS WHEREOF the parties have executed this Agreement as of the Effective Date.

LEA:

Signature: _____ Date: _____

Name / title: _____

Provider — Architecture of Grace:

Signature: _____ Date: _____

Name / title: _____

Exhibit A — Description of services

Tick the layers this Agreement covers. Layers not enabled create no Student Data.

Enabled	Layer	What it is	Student Data created
☐	1. Curriculum	Six companion novels, the lessons, anchor charts, scenario cards, worksheets, whole-class discussion, the Quiet Space and calming tools	None. Instruction.
☐	2. Academic practice	Activity pages in mathematics, science, social studies and English, with printable records	A practice record, only where a student sends one
☐	3. Check-in layer	The self-reflection; Daily Check-In; School-Day Exit Slip; Home Check-In; Home Observations; the adult team check-in; and This Is Me	Yes — see Exhibit B

The self-reflection, in detail

The self-reflection presents **nineteen statements**. **Eighteen are scored**, across three domains — Emotional Regulation & Well-Being; Self-Compassion & Growth Mindset; Social Competency & Repair. The nineteenth is a **closing safety statement**: it produces no score, and instead sets two flags and a closing word so that an adult knows to have a conversation. It runs in Quick and Thorough modes, in English and Spanish, and produces domain and composite values used as flags. **It is not diagnostic, is not independently validated, and is not for high-stakes decisions.**

Where product materials elsewhere refer to “18 items”, that is the count of **scored** items. Any consent or inspection copy must show all nineteen.

Exhibit B — Schedule of data

The two modes

Mode 1 — On device (default). Records are stored only in the browser on the device used. The identifier is a code, initials or seat number assigned by the educator. Nothing is transmitted. The Provider has no access.

Mode 2 — Synced to the LEA-controlled Destination. Completed records are transmitted over TLS and appended to the Destination, one row per record.

CLASS LINKS AND QR CODES ALWAYS SYNC A record opened through a generated classroom link or QR code syncs **whether or not** syncing is enabled on that device. Staff shall treat any shared link or posted QR code as a syncing mechanism.

What each record contains

Every row carries a timestamp and date, district, school and class identifiers, grade, term, and the educator-assigned student identifier. Beyond those:

Destination tab	Written by	Additional contents
-----------------	------------	---------------------

Responses	The self-reflection	Language; mode; three domain values; a composite; four comparison values; an internal tier and the words shown beside it; two safety flags ; a closing word; whether the taker is a K-12 student or an adult; whether taken at school or at home; and the eighteen scored item responses, eighteen intensity values and up to three optional written reflections.
DailyCheckins	Daily Check-In; This Is Me	Arrival; feeling words; readiness; need; connection; a challenge and its impact; a context tag; whether the student would tell an adult; agency; regulated / used a strategy / connected; a percentage; an optional note; a follow-up marker.
SupportCheckins	The adult team check-in	An adult's observation about a student, and the role and identifier of the adult who wrote it.
ExitSlips	School-Day Exit Slip	Best and hardest class with reasons; a good and a rough moment; a response; a closing; a word for the day; written text.
HomeObservations	A family member	Skill; level; time of day; activity; support given; an optional note.
HomeCheckins	Home Check-In	How morning, afternoon and evening went; what helped; an optional note.
Practice	Academic activity pages	Activity identifier and name; skill; set number; item count; independent and supported counts; percentage independent; number correct; hints used; a confidence rating. No score about the child as a person.

No names, dates of birth, contact details, government identifiers, biometric data or precise location are requested or stored by any instrument, unless the LEA deliberately configures a field to hold one. The design intent is pseudonymous use keyed to educator-assigned codes.

The public Voices comment wall

An optional public wall. A post carries an optional first name, a selected role and a short message; posts are stored in a separate Comments area of the Destination and shown publicly. Automated filtering blocks email addresses, telephone numbers, hyperlinks and common profanity, and caps length, but the wall is **open, not pre-moderated**. **The LEA decides whether to enable it and names who monitors it**. Posts are not Student Data.

Exhibit C — Known limitations and compensating controls

These limitations are disclosed so the LEA can design around them. Each compensating control is the LEA's to operate.

Limitation	Compensating control the LEA should adopt
The write key is public by design and allows forged rows that are indistinguishable from genuine ones. It cannot read, alter or delete.	Treat a surprising row as unverified. Rotate the key on any suspicion. Do not use synced rows as the sole evidence for a consequential decision about a student — which Article VI already requires.
The read key is not scoped : one key returns every row in the Destination.	One Destination per boundary that matters. If two schools must not see each other's data, give them two Destinations and two key pairs. Name the individuals who hold the read key, and record it.
No per-user authentication. The results view is gated by a convenience code, not a login.	Deploy on managed devices; restrict who holds the published links; treat the results view as a document, not an account. Where authenticated access is required, this product is not the right fit.
The site's default configuration may accept classroom links from any school identifier.	Narrow the permitted identifiers to the LEA's own — but only after regenerating every link and QR code and decoding one to confirm it carries its own destination.
The instrument is not independently validated .	Use it as a flag for conversation. Articles V and VI govern; do not use it in eligibility or programming decisions.
Records already synced are not removed when a device is cleared.	Deletion requests must be satisfied in the Destination, which the LEA controls and can edit directly.

Exhibit D — Provider practices summary

- Data is used only to provide the services; never sold, rented, or used for advertising or profiling.
- **Never used to train or improve any artificial-intelligence or machine-learning model**, and never disclosed to a third party for that purpose.
- Local by default. Transmission occurs only where the LEA enables it, over TLS, to a Destination the LEA owns.
- The Provider operates no back-end for LEA deployments and retains no synced Student Data.
- No student names are requested; use is pseudonymous, keyed to educator-assigned codes.
- The security posture, including its limits, is published rather than summarised — see Exhibit C and Annexes 1 and 2.
- The services are pilot-stage and not independently validated. Scores are flags for conversation, not diagnoses.

Exhibit E — State addendum

Complete for the LEA's jurisdiction. [Illinois shown as a worked example; confirm current statutory text with counsel.]

Item	Value
Governing statute(s)	[e.g. Illinois: 105 ILCS 85 (SOPPA); 105 ILCS 10 (Student Records Act)]

Provider's statutory role	[e.g. "operator" under SOPPA]
Breach notice: Provider → LEA	[_____ days], and in any event no later than the 72 hours in Article VIII
Breach notice: LEA → parents	[_____ days]
Minimum retention	[e.g. Illinois: five years for a temporary student record]
Maximum retention / destruction	[e.g. Louisiana: thirty days]
Records production deadline	[e.g. Illinois: ten business days]
Consent basis recorded by the LEA	[written opt-in / other, with counsel's determination attached]
Published list of operators required?	[yes / no]

Exhibit F — General offer of terms (optional)

Under the SDPC general-offer model the Provider may offer these terms to any additional LEA that accepts them by countersigning below, subject to that LEA's independent legal review and to completion of Exhibits A and E for its own configuration and jurisdiction.

Accepting LEA: _____

Signature: _____ Date: _____

Name / title: _____

Notes for the LEA's counsel

Four clauses in this template are the ones most likely to need negotiation. They are flagged rather than quietly drafted in the Provider's favour.

- **Article XII.6, liability cap.** A cap set at "fees paid in the preceding twelve months" resolves to zero where the services are provided at no charge. A fixed floor is offered as a bracketed alternative.
- **Article VIII.3, incidents inside the LEA's own Destination.** Because the Destination is LEA-owned, the LEA leads that response. Counsel should confirm this matches the LEA's insurance and policy.
- **Article V, consent.** The Provider takes a position on contested federal guidance and says so. The LEA should record its own determination rather than adopt the Provider's by default.
- **Exhibit C.** These are disclosed product limitations, not warranties. Counsel should satisfy itself that the compensating controls are operationally realistic for this LEA before signature.

Version 2.0. Written 6 September 2026 against sync script version 11 (5 September 2026). Supersedes the June 2026 template in full. Annex 1: Data & Privacy Statement v2.0. Annex 2: IT Deployment & Data Guide v2.0. Not legal advice.