
This Student Data Privacy Agreement (this “DPA”) is entered into between School Circle Network (“Provider”) and [the signing School or School Network] (“Local Education Agency” or “LEA”), and governs Provider’s handling of Student Data in connection with the School Circle Network platform (the “Service”).

RECITALS. WHEREAS, Provider operates the Service, a community platform used by Schools, School Networks, and Parent-Teacher Organizations to publish organizational content and by parents and staff to engage with it, as more fully described in the Platform Terms of Service; and WHEREAS, in the course of providing the Service, Provider may receive, create, or have access to limited Student Data as described in Exhibit A; and WHEREAS, the parties recognize the importance of protecting personally identifiable student information as required by the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. § 1232g (34 CFR Part 99), the Protection of Pupil Rights Amendment (“PPRA”) at 20 U.S.C. § 1232h, the Children’s Online Privacy Protection Act (“COPPA”) at 15 U.S.C. §§ 6501–6506 (16 CFR Part 312), and applicable state student data privacy laws; NOW THEREFORE, the parties agree to the Article and Exhibit provisions set forth below.

ARTICLE I: PURPOSE AND SCOPE

1.1. Purpose of DPA

The purpose of this DPA is to describe the duties and responsibilities of the parties with respect to Student Data processed through the Service, and to comply with applicable federal, state, and local student privacy laws. To the extent the LEA designates Provider a “School Official” with a legitimate educational interest under FERPA, and applicable law permits that designation, Provider will handle Student Data under the direct control and supervision of the LEA as set forth in this DPA.

1.2. Description of the Service

The Service and the categories of Student Data it may process on the LEA’s behalf are described in Exhibit A (“Schedule of Student Data”). If Provider adds a feature that changes the categories of Student Data processed, Provider will update Exhibit A and notify the LEA in accordance with Article VI, Section 6.5.

1.3. Student Data to Be Provided

Provider will process only the Student Data identified in Exhibit A. Student Data reaching the Service comes from two sources only: (a) a parent or guardian who voluntarily creates a profile for their own child within their own account, in order to use features such as volunteer sign-ups, team rosters, or membership registration tied to that child; and (b) where a School or School Network enables it, a teacher or staff member entering a class roster entry (name only) that a parent may later choose to claim and link to their own child’s profile — never automatically matched by name alone. The Service does not import student rosters from a student information system, does not issue a student their own login, and does not collect Student Data through any student-facing account.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

2.1. Student Data Property of the LEA

As between the LEA and Provider, all Student Data processed by Provider under this DPA is and remains the property of the LEA (or, where Student Data originates from a parent/guardian acting independently of any LEA direction, the property of that parent/guardian). Provider claims no ownership interest in Student Data.

2.2. Parent, Guardian, and Eligible Student Access

A parent or guardian may, at any time and without needing to go through the LEA, directly review, correct, or delete the profile they created for their own child within their own account. Where the LEA requests it to support the LEA's own obligations to parents, guardians, or eligible students under applicable law, Provider will provide the LEA with a copy of, or reasonable means to access, correct, or delete, a specific student's Student Data held by Provider, within thirty (30) days of the request or sooner if required by applicable state law.

2.3. Subprocessors

Provider may engage third-party service providers ("Subprocessors") to support operation of the Service, such as hosting, email delivery, or SMS providers. Provider will bind each Subprocessor that has access to Student Data to confidentiality and data protection obligations materially consistent with this DPA, including a prohibition on selling Student Data, and will remain responsible for each Subprocessor's handling of Student Data. A current list of Subprocessors is available on request to Provider's designated contact under Article VI, Section 6.6.

ARTICLE III: DUTIES OF THE LEA

3.1. Compliance with Applicable Law

The LEA will use the Service and provide or authorize Student Data in compliance with all applicable federal, state, and local student privacy laws, including obtaining any parental consent or providing any annual notification of rights required for its own use of the Service.

3.2. Reasonable Precautions

The LEA will employ reasonable administrative, physical, and technical safeguards to protect its representatives' account credentials from unauthorized access, disclosure, or use.

3.3. Breach Notification to Provider

The LEA will notify Provider within seventy-two (72) hours of any confirmed unauthorized access to the Service or Student Data originating from the LEA's own account, systems, or personnel, and will provide reasonable assistance to Provider in investigating and responding to it.

ARTICLE IV: DUTIES OF PROVIDER

4.1. Authorized Use

Provider will use Student Data solely to provide, maintain, secure, and improve the Service for the benefit of the LEA and its community, to provide customer support, to comply with applicable law, and for the limited, non-identifying uses described in Section 4.5. Provider will not use Student Data for any other purpose without the LEA's prior written consent.

4.2. Personnel Obligations

Provider will require every employee or contractor with access to Student Data to comply with the applicable provisions of this DPA and to be bound by a confidentiality obligation covering Student Data.

4.3. No Sale or Improper Disclosure

Provider will not sell Student Data, and will not disclose Student Data to any third party except: (a) to Subprocessors under Article II, Section 2.3; (b) as directed or permitted by the LEA or a parent/guardian acting on their own child's profile; (c) to protect the safety of users or others, or the security or integrity of the Service; (d) as De-Identified Data under Section 4.5; or (e) pursuant to a valid judicial order, subpoena, or other lawful legal process, in which case Provider will give the LEA advance notice of the compelled disclosure where legally permitted to do so.

4.4. No Targeted Advertising

Provider will not use, disclose, or sell Student Data to inform, influence, or enable targeted advertising to a student, or to build a commercial profile of a student for any purpose other than providing the Service. This section does not prohibit Provider from notifying account holders about Service updates that are not targeted advertising.

4.5. De-Identified Data

Provider may create and use De-Identified Data — Student Data from which all personally identifiable information has been removed or obscured such that the remaining information does not reasonably identify a specific individual — for product improvement, aggregate usage reporting, and research purposes. Provider will not attempt to re-identify De-Identified Data, and will not transfer it to a third party unless that party agrees in writing not to attempt re-identification. Provider's use of De-Identified Data survives termination of this DPA.

4.6. Disposition of Data

Upon the LEA's written request, or within sixty (60) days of termination of this DPA, Provider will delete or de-identify Student Data obtained under this DPA, except for data retained in routine backups for a limited period (which will be deleted or de-identified on the same schedule once those backups expire) or as otherwise required by law. This obligation does not extend to De-Identified Data or to content a student or parent/guardian has affirmatively exported or transferred out of the Service into their own possession.

ARTICLE V: DATA SECURITY AND BREACH PROVISIONS

5.1. Data Storage

Student Data is stored on infrastructure located in the United States. Provider will notify the LEA before Student Data is stored outside the United States on an ongoing basis.

5.2. Data Security

Provider maintains a written information security program with administrative, technical, and physical safeguards designed to protect Student Data against unauthorized access, disclosure, alteration, or destruction, including encryption of Student Data in transit, access controls limiting Student Data access to personnel with a legitimate need, and periodic review of its security practices against generally accepted industry standards.

5.3. Security Audits

No more than once per contract year, or following a confirmed Data Breach, the LEA may request a reasonable written summary of Provider's security practices relevant to the Service, upon at least ten (10) business days' notice and execution of an appropriate confidentiality agreement.

5.4. Data Breach Notification

If Provider confirms unauthorized access to or disclosure of Student Data that compromises its security, confidentiality, or integrity (a "Data Breach"), Provider will notify the LEA without unreasonable delay and in no event later than seventy-two (72) hours after confirmation, unless a law enforcement investigation requires a delay, in which case notice will follow as soon as the delay is no longer required. The notice will include, to the extent then known: the nature and estimated date of the Data Breach, the categories of Student Data reasonably believed affected, and the steps Provider is taking in response. Provider will not itself notify affected individuals, regulators, or other third parties about a Data Breach without first notifying the LEA, except where required by law.

ARTICLE VI: TERM, TERMINATION, AND GENERAL PROVISIONS

6.1. Term

This DPA takes effect on the date it is executed and remains in effect for as long as Provider retains Student Data under this DPA, whether or not the underlying Platform Terms of Service or Services Agreement remains active.

6.2. Termination

Either party may terminate this DPA by written notice if the underlying Service relationship has lapsed or been terminated, or if the other party materially breaches this DPA and does not cure that breach within thirty (30) days of written notice. Termination of this DPA triggers Provider's disposition obligations under Article IV, Section 4.6.

6.3. Governing Law; Venue

This DPA is governed by the laws of the State of New Jersey, without regard to conflict-of-laws principles. Each party consents to the exclusive jurisdiction of the state and federal courts located in New Jersey for any dispute arising out of or relating to this DPA, except that a dispute otherwise subject to the arbitration provision of the Platform Terms of Service remains governed by that provision.

6.4. Priority of Agreements

With respect to the treatment of Student Data specifically, this DPA governs over any conflicting term of the Platform Terms of Service or a Services Agreement between the parties. In all other respects, the Platform Terms of Service and any Services Agreement remain in full force and effect.

6.5. Amendment; Notices

This DPA may be amended only by a new version executed by both parties through the School Circle Network platform or by a signed writing. Notices under this DPA must be given in writing to the addresses or account contact information on file for each party, or to <https://schoolcircle.net/contact> for Provider, and are deemed given when delivered by email with confirmation of receipt.

6.6. Electronic Signatures

This DPA is executed electronically by an authorized representative of the LEA through the School Circle Network platform, and countersigned by Provider's authorized signatory upon review, as reflected in the execution record associated with this DPA. Each party agrees that its electronic signature is the legally binding equivalent of a handwritten signature and will not contest the validity of this DPA on the grounds that it is an electronic record.

ARTICLE Exhibit A: SCHEDULE OF STUDENT DATA

A.1. Categories of Student Data Processed

Category	Elements	Collected?
Student Identifiers	First name (always), and either a full last name or just a last initial (the entering parent/guardian or teacher chooses), plus a Provider-assigned internal record ID	Yes — as entered by a parent/guardian, or by a teacher/staff member on an unclaimed roster entry; a full legal last name is never required by the Service
Enrollment	School affiliation, grade level, team/roster affiliation	Yes — as entered by a parent/guardian
Student Login Credentials	Username, password, student-specific account	No — students do not have their own account or login; a parent/guardian's own login controls their child's profile
Communications	Direct messages to or from a student, in-app student chat	No — the Service has no student-facing messaging feature
Assessment / Academic Performance	Grades, test scores, behavior/conduct points, feedback logs	No — the Service has no classroom feedback, grading, or behavior-tracking feature
Health / Biometric	Medical alerts, disability information, fingerprint/facial recognition	No, and the LEA should not submit any such information through the Service
Transportation / Attendance	Bus assignment, pickup/drop-off, daily or class attendance	No
Application Technology Metadata	IP address, cookies, device/browser information	Only at the parent/guardian account level (never a student-specific record) — see the School Circle Network Cookie Policy

A.2. How Student Data Reaches the Service

Student Data is never imported from an LEA's student information system, and no rostering or single sign-on integration exists. Every student record either (a) is created directly by a parent or guardian inside their own account, for their own child, and can be edited or deleted by that parent or guardian at any time; or (b) begins as a name-only entry a teacher or staff member adds to a class roster, which has no effect until a parent or guardian affirmatively claims it as their own child — an unclaimed roster entry is never treated as, or disclosed as, a specific identified student's data.

A.3. Purpose of Processing

The Student Data described above is used only to power the specific features a parent/guardian or School/School Network chooses to use — for example, associating a volunteer sign-up, a sports team roster, a membership registration, or a shop order with the correct child — and for the security, support, and improvement purposes described in Article IV.

A.4. Name Minimization — Why Only a First Name and Last Name or Last Initial

What is collected. A student record on the Service requires only a first name, plus a last name or a last initial — a full legal last name is not itself required, and no middle name, suffix, date of birth, or government identifier is ever requested. **Why.** The Service only ever needs enough of a name to let the entering parent/guardian, or the School/School Network staff maintaining a class roster, tell one child apart from another within their own household or classroom — it has no purpose that requires a student's full legal identity. **How it is used.** Whichever name a parent/guardian or teacher enters is what appears wherever that specific record is used (a roster, a volunteer sign-up, a shop order) — it is never independently verified against, expanded from, or reconciled with any government or school-system record. **Recommendation, not a requirement.** Because this field is free text entered by the parent/guardian (or by a teacher on an unclaimed roster entry a parent must still claim), a parent/guardian who prefers not to enter a full last name may enter just a first name and last initial instead (for example, "Emma S." rather than "Emma Smith") — the Service functions identically either way, and Provider does not require, request, or reject either format.

ARTICLE Exhibit B: DEFINITIONS

“Data Breach” means a confirmed unauthorized access to, disclosure of, or acquisition of Student Data that compromises its security, confidentiality, or integrity. **“De-Identified Data”** means Student Data from which all personally identifiable information has been removed or obscured such that the remaining information cannot reasonably be used to identify a specific individual. **“Education Records”** has the meaning given in FERPA, 20 U.S.C. § 1232g(a)(4). **“Local Education Agency” or “LEA”** means the School or School Network that executes this DPA. **“Personally Identifiable Information”** means any information that is linked or reasonably linkable to an identified or identifiable individual. **“School Official”** has the meaning given in 34 CFR § 99.31(b), to the extent that designation is used by the LEA with respect to Provider. **“Student Data”** means Personally Identifiable Information relating to a student that is provided to Provider by or at the direction of the LEA, or created or provided by a student’s parent or guardian through the Service, as further described in Exhibit A. Student Data does not include De-Identified Data, or information a parent or guardian provides independent of any School or School Network affiliation. **“Subprocessor”** means a third party engaged by Provider that has access to or stores Student Data in order to help operate the Service. **“Targeted Advertising”** means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or on that student’s activity on the Service over time.

Signature

Print, sign, and return this page to School Circle Network to have your offline signature recorded — printing and signing this page does not by itself execute the agreement.

Signature	Date
-----------	------

Printed Name

Title

Organization

Document content hash (sha256): e9e9ca4f578e5b4225b6e43c21d48b57e1a558175f1bb760577ca565f0e4626d