Where School Community Connects

Security & Trust

Updated September 17, 2026

School Circle Network uses account authorization, CSRF protection, audit records, and policy acceptance records as part of its application safeguards. No website can promise absolute security.

Report a concern

Do not include passwords, payment card details, or sensitive student information in an initial report. Contact or use the contact page.

Certifications

Only currently active, administrator-verified certifications appear below. An empty list means the site is making no certification claim.

Account Protection You Can Use

Beyond your password, your account supports two-factor authentication (an authenticator app) and passkeys (device-based sign-in using Face ID, Touch ID, Windows Hello, or a security key) as optional, stronger sign-in methods. You can review your recent login history and manage which devices are remembered as trusted from your own Account Security settings, and remove any device you no longer recognize.

How Sensitive Files Are Protected

Uploaded files that are not meant to be public — verification documents submitted to claim an organization page, and signature images used for institutional agreements — are stored in directories that deny all direct web access. They are only ever readable through a specific, authorization-checked page (for example, a generated agreement PDF, or an admin review screen), never through a guessable or public URL.

Payment Security

Full payment card details are never entered into, or stored on, School Circle Network's own servers. Card payments are handled directly by Stripe or PayPal, and School Circle Network stores only the transaction metadata (amount, date, status) needed for receipts, refunds, and accounting.

Message Encryption

Messages you send through Messenger are encrypted at rest — stored using AES-256-GCM encryption rather than as plain text, so a raw database dump or an exposed backup file does not casually expose conversation content. To be clear and not overclaim: this is not end-to-end encryption. The Service decrypts a message server-side to display it to an authorized participant, using an installation-wide key that is never shipped in code or sent to any client, and there is deliberately no admin interface for browsing message content outside of a user-initiated abuse report. We use this design, rather than true end-to-end encryption, specifically so your message history is available the same way on every device you sign into, with no separate key or PIN to set up or risk losing.

If We Confirm a Security Incident

If we confirm unauthorized access to or disclosure of your personal information, we will notify affected users without unreasonable delay, consistent with applicable law — the same commitment reflected in our institutional Student Data Privacy Agreement for organizations that have executed one.

Authoritative HTML source: https://schoolcircle.net/legal/security-trust
Downloaded November 15, 2026