Security & Privacy Whitepaper

TIERSPRING · STUDENT SUCCESS CASE MANAGEMENT FOR MACOS & WINDOWS

For district technology and student-privacy officers evaluating Tierspring.
Version 0.9 (draft) · August 2026 · Vendor entity: *[to be formed]*

The one-sentence summary: Tierspring is software your district runs, not a service that holds your data. Student information never reaches the vendor — because there is nowhere for it to go.

1 · The architecture, in one paragraph

Tierspring is a native macOS application installed on a district-managed Mac. All student data lives in a single SQLite database file on that Mac, inside the signed-in user's Library folder. The application makes **no outbound network requests**: there is no server component, no cloud synchronization, no vendor account, no analytics, no crash reporting, and no telemetry of any kind. A strict Content Security Policy and a narrow, allow-listed process boundary separate the user interface from data access. The vendor cannot see, receive, or recover any district data — a claim your team can verify directly (section 7).

2 · Why this matters for procurement

- **No data-sharing relationship exists.** Because no student data is transmitted to or stored by the vendor, Tierspring operates as purchased software rather than an outsourced service holding education records. Districts that use the SDPC national Data Privacy Agreement can typically execute it with nearly every data-transfer exhibit marked not-applicable.
- **FERPA posture:** education records stay inside the district's own device-management and account controls at all times, exactly like records in a district file share. The "school official" analysis that cloud tools require has almost no surface here.
- **Breach surface:** there is no vendor system to breach. The threat model reduces to the physical device — which the district already manages (section 4).
- **No integration credentials.** Tierspring imports from files the district already exports (SIS report PDFs, CSV). It never asks for SIS, SSO, or Google credentials.

3 · Data inventory and location

DATA	LOCATION	LEAVES THE DEVICE?
All student records (the database)	`~/Library/Application Support/Tierspring/` on the specialist's Mac	Never
Backups	A district-chosen folder or drive	Only where the district puts them
Exports and PDFs	Wherever the user saves them	User-initiated only
Vendor-held student data	**None. There is no vendor data store.**	

Optional companions (a staff referral form, a check-in/check-out score form) run as Google Forms and Apps Script *inside the district's own Google Workspace tenant*, created and owned by district accounts. Data submitted there is district data in district systems, governed by the district's existing Google Workspace agreement; Tierspring imports it via a CSV the district exports. The vendor has no access to these forms.

4 · Device-level protection

- **Encryption at rest** is provided by macOS FileVault, which the deployment guide requires. The application deliberately relies on FileVault rather than shipping its own cryptography — full-disk encryption managed by the district's MDM is stronger and auditable.
- **Application lock:** an optional password (scrypt-hashed, random per-install salt, constant-time verification, never stored in any recoverable form) locks the interface, with configurable auto-lock on idle.
- **Privacy display mode** reduces on-screen names to initials for shared-screen situations, and a dashboard privacy option suppresses sensitive counts on the most-often-visible screen.

5 · Accountability inside the app

- **Audit history:** creations, edits, imports, risk overrides, and settings changes are logged and reviewable in the app.
- **Note revisions:** editing a case note preserves every prior version. Records show what was known when.

- **Explainable scoring:** the risk score is a transparent, district-configurable rule set — every point traces to a named factor and its evidence, and any score can be overridden with a documented reason. No opaque models, no third-party AI processing of student data.
- **Soft deletion:** records archive rather than silently disappear.

6 · Software integrity

- Signed with an Apple **Developer ID** and **notarized by Apple** (Gatekeeper verdict: *Notarized Developer ID*), with the macOS hardened runtime enabled.
- Updates are distributed as full signed installers; nothing self-updates over the network in the current release, so the district controls exactly which version runs.
- Dependency surface is deliberately small (an Electron shell, SQLite, and a PDF/QR library — no networking, analytics, or advertising SDKs).

7 · Verify it yourself

Districts should not take a vendor's word for "no data leaves the device." Suggested verification, each taking minutes: run the app under `nettop` or Little Snitch and observe zero outbound connections; inspect `~/Library/Application Support/Tierspring/` and confirm all data is local SQLite; review the Gatekeeper assessment with `spctl --assess -v /Applications/Tierspring.app`. A code-review copy can be made available under NDA for district security review.

8 · Honest limitations

> - **Single user by design.** Tierspring is the specialist's caseload tool. It has no multi-user access control; a district needing shared, role-based access to the same live records needs a different class of product (and the server, agreements, and breach surface that come with it).
> - **The database is not application-encrypted.** FileVault is required, not optional. Anyone with the Mac's user account can read the data — identical to the district's existing stance on local documents.
> - **The app password has no recovery.** This is a deliberate security property, and it means the password belongs in the district's password manager.
> - **Backups are the district's responsibility**, and exported files (PDFs, CSVs) leave the app's protections the moment they are created — normal records-handling policy applies.

9 · Compliance quick reference

QUESTION DISTRICTS ASK	ANSWER
Where is student data hosted?	Nowhere — on the district's own Mac only. No vendor hosting exists.
Does the vendor access PII?	No. The vendor has no technical means of access.
Sub-processors?	None. No data is processed off-device.
Data deletion on termination?	The district deletes the local database; nothing to request from the vendor.
Breach notification?	Vendor-side breach of student data is not possible; device-side incidents follow the district's existing device policy.
Student data sold or used for advertising / AI training?	Never; also technically impossible — the vendor never receives it.
SOPIPA / state student-privacy laws	Obligations largely attach to operators who collect or maintain student data; Tierspring's vendor does neither. Written assurances provided on request.

> **Contact.** Questions, verification requests, or the code-review process: *[vendor contact — to be completed at entity formation]*.