sachi

BRIEFING NOTE

The signature behind Exhibit D

Every provider selling into a US school district signs a student data privacy agreement. Most sign the National Data Privacy Agreement, and at the end of it sits a form certifying that student data was disposed of. **Signing creates direct obligations on the vendor:** the provider becomes a School Official under FERPA, acting under the district's control, and takes on disposition duties owed contractually to the district. Nothing in the NDPA specifies what evidence stands behind that certification.

What the NDPA actually asks for

Exhibit D	Closes with a signature block headed **Notice of Verified Disposition of Data**, executed by authorised representatives of both district and provider. The provider certifies that student data was destroyed, transferred, or de-identified.
§1.1 & Exhibit C	The provider acts as a **School Official** under FERPA, under the district's direct control for the use and maintenance of student data. The district remains accountable for its records; the provider takes on its own duties by contract.
§4.6	Disposition within **60 days** of a written request, and again within 60 days of termination. A district may require the provider's retention and disposition practice in writing, at any time.
Exhibit C	Student Data is defined to include data **"gathered, created, or inferred"** by the provider. Inferred data is in scope — reaching learner profiles, behavioural models and embeddings derived from a student's activity, not only the records a student typed.
Exhibit B	The standard schedule of data lists **voice recordings** as a collectable category. Under the amended COPPA Rule, a voiceprint is treated as a biometric identifier and is personal information.

The form asks a provider to certify disposition.
It never asks how disposition was verified.

That is not a defect in the NDPA. Contracts allocate obligations; they do not specify engineering. But it does mean the strength of the certification rests entirely on what the provider can show.

Why certifying is harder than it looks

Inferred data

Deleting a student's records leaves the embeddings, profiles and model state derived from them — Student Data by the agreement's own definition.

Backups

A 30 or 90 day rotation means a restore can resurrect a student disposed of last month. Reaching backups is where most deletion routines stop.

Subprocessors

§2.3 requires subprocessors be bound to terms no less stringent. Disposition has to propagate to every vendor holding a copy.

The attestation is not tested in the ordinary course. It is tested after an incident.

In practice a signed Exhibit D is rarely questioned at the time. Where practitioners report it surfacing is after a breach: when data appears that should have been disposed of, the certification stands as the record of what was represented, and by whom.

What provable disposition looks like

Chasing every copy of a student's data across databases, indexes, warehouses and backups is difficult to do and harder still to evidence. Encrypting per student and destroying the key inverts it: one act, one record, every copy unreadable at once.

We hold the keys. We never hold the data.

Student data is encrypted by our SDK inside your application, before it is first written, and stored as ciphertext in **your own infrastructure**. Sachi holds only the per-student keys — so adopting us narrows your subprocessor surface rather than widening it, and a breach of Sachi exposes no readable student record.

YOUR SYSTEMS	SACHI
Plaintext in memory during a session. Ciphertext at rest — records, embeddings, backups.	Keys, consent state, retention policy, audit chain. No student data, ever.

One call, and the evidence is generated

```
# Disposition on request — or automatically at retention expiry
resp = sachi.students.delete(
    student_id="stu_84f2",
    reason="lea_disposition_request",
)

# => status: "key_destroyed" · scope: records, embeddings, backups
#   objects_unreadable: 1284 · completed_at: 2026-08-18T14:22:07Z
#   certificate_url: "api.getsachi.ai/v1/certificates/a7f3..."
```

Against the agreement

NDPA OBLIGATION	WHAT A PROVIDER CAN SHOW
Exhibit D — Notice of Verified Disposition	A signed certificate naming subject, method, scope and timestamp, referenced to a tamper-evident log entry rather than to an assertion.
§4.6 — disposition within 60 days	Key destruction is a single operation, with its completion time recorded. Retention expiry is enforced on every stored item rather than run as a periodic sweep.
Exhibit C — inferred data in scope	Embeddings and derived profiles are encrypted under the same per-student key, so they die with it. Nothing is hunted down separately.
§5.3 & Exhibit F — recognised framework	Cryptographic erasure is a recognised media sanitisation technique in NIST SP 800-88, the standard the NIST frameworks listed in Exhibit F draw on for sanitisation controls.

Three questions worth asking internally

- → When we sign Exhibit D, what could we produce if a district asked how disposition was verified?
- → Does our deletion routine reach inferred data — embeddings, profiles, model state — or only source records?
- → If a backup were restored tomorrow, would a student we disposed of last month come back?

> **The API is available for drop-in technical pilots.** If those questions are worth an hour of an engineer's time, we are running a small number of scoped pilots with teams selling into districts.

Kalei Biehl · kalei@getsachi.ai · getsachi.ai | COPPA liability is non-delegable; the operator remains responsible for its own compliance. Not legal advice. Sources: NDPA Standard v2.2 (Access 4 Learning / SDPC); 16 C.F.R. Part 312; NIST SP 800-88 Rev. 1.