

Your Ed Law 2-d Cheatsheet



Prepared by [Michelle Krieger](#), DPO, Lake Shore Central Schools | Co-author, From Chalk Dust to Digital Trust
In partnership with Virtru
Read Michelle's Newsletter, [The Privacy Post](#)

Top 5 To-Do's

- 1 Audit Local Downloads for Unencrypted Files**
Clear student roster exports, evaluation reports, and spreadsheets sitting unprotected on local desktops, downloads folders, or flash drives. Ed Law 2-d requires protection at rest, not just in transit.
- 2 Brief Staff on Digital Footprints**
Work emails, chat logs, and ticket systems are official records. They are subject to public disclosure, data requests, and LGS-1 retention requirements. "Deleted" does not mean "eligible for disposition."
- 3 Create a Fast-Track App Approval Process**
Give teachers a simple intake form for app and AI tool requests. Shadow EdTech is a breach vector. Make the right path the easy path.
- 4 Trigger Deletion Requests for Cancelled Software**
Identify platforms the district stopped paying for. Formally request student data purges. Confirm LGS-1 disposition eligibility for those record types first.
- 5 Run a 30-Minute Executive Tabletop**
Schedule a mock-breach scenario with your Superintendent, IT Director, Legal Counsel, and PR lead. Build it around the 10-calendar-day notification clock. That timer starts the moment anyone in the district learns of an incident.

Extra Mile

Verify At-Rest Encryption in Writing
TLS in transit is not enough. Ask vendors to confirm data is encrypted in their databases and backups too.

Set a 4-Hour Internal Escalation Rule
Any suspected breach or lost device gets reported to IT and the Superintendent within 4 hours. Vendors have up to 7 days to notify you. That can leave the district with as few as 3 days on the NYSED clock.

Request Subprocessor Lists
Ask your top EdTech vendors who else receives district data. Third-party incidents now account for nearly 1 in 3 K-12 breaches.

Standardize Parent ID Verification
Front-office staff need a step-by-step identity check before releasing any student or staff records. Under Part 121, unauthorized access is reportable, even if no data was taken.

Pre-Fill Your Incident Reporting Forms
NYSED uses one consolidated electronic form, updated January 2026. Pre-draft it with your district's standing details now. Not during an active incident.

Key References

LGS-1 Retention Schedule
archives.nysed.gov

NYSED Incident Reporting Form
nysed.gov/data-privacy-security



Learn how districts operationalize Ed Law 2-d at virtru.com