DISTRICT GOVERNANCE CHECKLIST

Five Governance Questions Every District Should Be Able to Answer Now

Use this checklist to assess your current governance posture and identify gaps before your next audit, incident, or board review.

1. Where Does Sensitive Student and Staff Data Live Today—And Who Can Access It?

If you can't map your data, you can't govern it. Many districts know their SIS and LMS, but not the full landscape: assessment platforms, counseling tools, AI apps, cloud drives, and third-party analytics that all touch student information.

What you should be able to show:

- ☐ A current inventory of systems that store or process student/staff data.
- ☐ Clear ownership for each system (program owner, technical owner, privacy owner).
- ☐ Role-based access lists showing who has view, edit, export, and admin rights.
- ☐ Documentation of any cross-border data flows or external hosting.

> **Notes:**
>
> _____
>
> _____
>
> _____

Status: ☐ Complete ☐ In Progress ☐ Not Started

2. Which AI and EdTech Tools Are Approved, Under What Conditions, and Where Are the Gaps?

AI adoption is moving faster than policy in many districts. Teachers are using chatbots, writing assistants, and lesson planners; students are using similar tools at home. Without a clear approval framework, you risk inconsistent practice, hidden data sharing, and unmanaged vendor relationships.

What you should be able to show:

- ☐ A published list of approved AI/edtech tools, by use case (instruction, planning, intervention, etc.).
- ☐ The specific conditions for each tool: grade bands, subjects, data types allowed, and required training.
- ☐ A documented process for requesting, reviewing, and approving new tools mid-year.
- ☐ Visibility into where controls are missing (e.g., tools in use but not approved, or approved but not configured safely).

> **Notes:**
> _____
> _____
> _____

Status: ☐ Complete ☐ In Progress ☐ Not Started

3. Can We Prove that Vendor Contracts and Data Protections Match What's Actually Happening in Our Systems?

A strong contract is only as good as your ability to verify it. Many districts have solid DPAs and FERPA language on file, but no easy way to confirm that vendors are honoring data minimization, retention limits, or “no model training” commitments in practice.

What you should be able to show:

- ☐ Current contracts and DPAs linked to each active system.
- ☐ Key data protection commitments (retention schedules, deletion timelines, subprocessor lists, training restrictions).
- ☐ Technical or operational verification that those commitments are being met (e.g., logs, reports, audit results).
- ☐ A process for re-certifying vendors annually or after major incidents.

Notes:

Status: ☐ Complete ☐ In Progress ☐ Not Started

4. Do We Know How Student Data Moves Between Systems, and Where It Could Be Overexposed?

Data doesn't sit still. It flows from SIS to LMS to assessment platforms to AI tools and back again. Every handoff is a potential risk point: over-broad exports, unnecessary fields, long retention in downstream systems, or unclear deletion responsibilities.

What you should be able to show:

- ☐ Data flow diagrams for your highest-risk use cases (rostering, grade sync, AI writing tools, etc.).
- ☐ Documentation of what fields move, why they're needed, and how long they're kept in each system.
- ☐ Use of minimization (e.g., tokenized IDs instead of full PII where possible).
- ☐ A plan to reduce or eliminate unnecessary data sharing.

Notes:

Status: ☐ Complete ☐ In Progress ☐ Not Started

5. If There's an Incident or an Audit Request, Can We Respond Quickly with Clear, Defensible Documentation?

Incidents and audits don't wait for convenient timing. When a parent asks about data access, a regulator requests documentation, or a breach hits a vendor, your team needs to respond with confidence, not scramble through emails and shared drives.

What you should be able to show:

- ☐ A single source of truth for policies, contracts, data maps, and access records.
- ☐ Pre-built reports for common requests (who accessed X student's data, which tools were used in Y classroom, etc.).
- ☐ Documented incident response steps, roles, and communication templates.

☐ Evidence of regular testing (tabletop exercises, access reviews, vendor recertifications).

Notes:

_____

_____

_____

Status: ☐ Complete ☐ In Progress ☐ Not Started

Next Steps

Assign an owner to each question above.

Set target dates to close identified gaps.

Revisit this checklist quarterly or after major incidents.