K–12 Application Approval Process Checklist

Quick Reference Guide for District Leaders and IT Teams

☐ Process Foundation

- ☐ Establish formal district approval process requiring evaluation before any app receives student data
- ☐ Create one standardized digital request form published on staff portal
- ☐ Prohibit informal approvals via email, chat, or verbal requests

☐ Data Collection & Minimization

- ☐ Capture intended use, target population, user scope, and specific data categories needed
- ☐ Require written justification for each requested data field
- ☐ Ask: Can app operate with tokens/anonymized attributes instead of raw PII?
- ☐ Document the "why" for all data requests and store for audits

☐ Governance & Review

- ☐ Establish cross-functional governance team (IT, curriculum, legal, leadership)
- ☐ Define RACI matrix clarifying decision-making authority
- ☐ Review policy alignment, data protection, data location/sovereignty, and vendor reputation
- ☐ Communicate decisions within 5–10 business days with clear outcomes: Approved, Approved with reduced scope, Deferred, or Declined

☐ Implementation

- ☐ Default to minimal data sharing—avoid "send everything" approaches
- ☐ Use curated data views or tokenized outputs instead of raw SIS access
- ☐ For pilots, use zero-PII trials with test/anonymized data
- ☐ Create searchable app record documenting purpose, data shared, legal basis, storage location, and retention expectations

☐ Lifecycle Management

- ☐ Make approvals time-bound: review pilots after one term, established tools annually
- ☐ Require explicit re-approval at each review cycle
- ☐ Document exit plan: what happens to data when contract ends
- ☐ When offboarding: revoke access, terminate feeds, verify vendor deletion, remove from catalogs, update documentation

☐ Culture & Continuous Improvement

- ☐ Keep request form simple; push technical questions to governance review
- ☐ Provide easy-to-search approved app catalog for staff
- ☐ Offer scenario-based training referencing real edtech privacy failures
- ☐ Emphasize "yes, safely" culture enabling tools while minimizing data exposure
- ☐ Monitor for shadow IT and direct staff into formal approval pathway
- ☐ Track metrics: approval turnaround time, apps retired, data fields reduced over time