BRIGHTBRIDGE LEARNING INTERNATIONAL

AI Use, Procurement & Vendor Due-Diligence Standard

Controls for external AI tools, embedded AI features, contract requirements, and exit planning

International Children's Education Nonprofit | Simulated AI Governance Consulting Engagement

Portfolio note
All organizational details, AI systems, roles, risks, scores, and data in this portfolio artifact are fictional or synthetic and are provided solely to demonstrate applied AI governance consulting methodology.

Version 1.0 | August 2026

1. Purpose and Policy Statement

BrightBridge must evaluate AI before purchase, pilot, activation, or material expansion. Procurement approval does not substitute for AI governance approval, and a vendor's assurance does not substitute for BrightBridge's responsibility to assess child safety, privacy, fairness, security, and human oversight.

No shadow AI
Business teams may not activate AI features, use consumer AI with restricted BrightBridge data, or sign AI-enabled vendor contracts outside the intake and due-diligence process.

2. AI Intake Workflow

1. Business sponsor submits AI intake questionnaire.
2. AI Governance Lead determines whether the capability is AI and creates an inventory record.
3. Preliminary risk tier is assigned.
4. Required reviewers are triggered: safeguarding, privacy, security, legal/compliance, accessibility, model/fairness, procurement/vendor risk.
5. Vendor evidence is collected and assessed.
6. Contract requirements are negotiated according to tier.
7. Controls and approval conditions are documented.
8. Appropriate authority records Approved, Approved with Conditions, Additional Assessment Required, or Rejected.
9. System enters monitoring and annual/vendor-change reassessment.

3. BrightBridge Prohibited / Restricted Procurement Uses

- AI intended for social scoring of children or families.
- AI that performs fully automated safeguarding case closure or denial of core support.
- AI that exploits child vulnerability through manipulative persuasion or dependency.
- AI with insufficient transparency for a High-risk use where BrightBridge cannot obtain necessary evidence or audit rights.
- AI that requires unrestricted vendor use of child or safeguarding data for generalized model training.
- Consumer AI accounts used with restricted, child, safeguarding, credential, or other sensitive BrightBridge data.

4. Vendor Due-Diligence Questionnaire

Domain	Due-Diligence Question
System & Ownership	Describe the AI functionality, model(s), provider(s), and any embedded third-party/foundation models.
System & Ownership	What is the intended use, known limitations, and prohibited use stated by the vendor?
System & Ownership	How are model versions identified and communicated to customers?
Data	What customer data is processed, stored, logged, or used for training/improvement?
Data	Can BrightBridge opt out of model training on its data? Is opt-out contractual and technically enforced?
Data	What categories of child, education, safeguarding, employment, donor, or sensitive data are supported or prohibited?
Data	Where is data stored and processed? List countries/regions and subprocessors.
Data	What retention periods apply to prompts, outputs, logs, embeddings, files, and backups?
Data	How is deletion verified at contract exit or request?
Security	Describe authentication, access control, encryption, tenant separation, logging, and incident response.
Security	Provide relevant security assurance reports or certifications and

Domain	Due-Diligence Question
	scope/limitations.
Safety	What safety evaluations have been performed for child-facing or vulnerable-population use?
Safety	What content safety, prompt-injection, misuse, and harmful-output controls exist?
Safety	How can BrightBridge configure or strengthen safety settings?
Fairness	What fairness/bias evaluations have been performed and for which populations, languages, or use cases?
Fairness	Can BrightBridge test subgroup outcomes or access sufficient output/logging to do so?
Performance	What performance metrics, validation data, and known failure modes are documented?
Performance	How does the vendor monitor drift, regressions, and model updates?
Transparency	What documentation is available: system card, model card, data sheet, evaluation report, change log?
Transparency	Can the vendor explain key factors or provide reason codes for consequential outputs?
Human Oversight	What controls support human review, override, escalation, and audit trails?
Human Oversight	Can BrightBridge prevent fully automated decisions in High-risk workflows?
Incident	What constitutes a vendor AI incident and how quickly will BrightBridge be notified?
Incident	Will the vendor share root-cause analysis, affected versions, remediation, and customer actions?
Subprocessors	List subprocessors/foundation model providers and notice/change process.
Contract	Will the vendor accept child-data restrictions, purpose limitation, confidentiality, and no-training commitments?
Contract	Will the vendor provide material model-change notification before or promptly after change?
Contract	Will the vendor grant audit/evaluation rights proportionate to risk?
Contract	What service levels or remedies apply to critical incidents or sustained performance/safety failures?
Exit	Can BrightBridge export necessary data, logs, decisions, and documentation at exit?
Exit	How are data deletion, model access, tokens/keys, and residual integrations closed?
Accessibility	What accessibility standards/testing apply to child-facing interfaces?
Localization	What languages and regions are validated? How are cultural/localization limitations documented?
Business Continuity	What happens if the AI service or underlying model becomes unavailable?
Governance	Who is the vendor's accountable owner for AI risk, safety, privacy, and customer escalation?

5. Minimum Contract Requirements by High-Risk Vendor

Requirement	BrightBridge Contract Expectation
Purpose limitation	Use BrightBridge data only to provide contracted services and agreed support functions.
No generalized model training	No training or improvement of generalized models using BrightBridge restricted/child/safeguarding data without explicit written approval.

Requirement	BrightBridge Contract Expectation
Child-data restrictions	Vendor must comply with BrightBridge approved data categories and prohibit unsupported sensitive uses.
Subprocessor transparency	List subprocessors/foundation model providers and provide notice of material changes.
Material model-change notice	Notify BrightBridge of changes that may affect performance, safety, data use, or controls.
Incident notification	Critical incident notice within contractually defined timeframe with follow-up root-cause analysis.
Audit/evaluation rights	Permit evidence review, customer testing, or independent assurance appropriate to risk.
Retention and deletion	Define retention and provide deletion confirmation at exit or on request.
Security	Maintain agreed security controls and promptly address material vulnerabilities.
Exit and portability	Support export, transition, access revocation, and evidence of residual data deletion.

6. Procurement Decision Standard

Decision	Criteria
APPROVED	Risk is Low/Moderate and required controls/evidence are complete.
APPROVED WITH CONDITIONS	Specific control gaps must close by due dates; monitoring or scope restrictions apply.
ADDITIONAL ASSESSMENT REQUIRED	High-risk use or evidence gaps require deeper impact, privacy, security, fairness, or safeguarding review.
REJECTED	Use is prohibited, vendor evidence is insufficient for risk, contract terms are unacceptable, or risk cannot be adequately controlled.

7. Annual and Event-Driven Vendor Reassessment

- Annual reassessment for High-risk vendors; risk-based for Moderate vendors.
- Reassess after material model release, new foundation model/provider, new data use, new country, safety incident, security incident, or material performance regression.
- Review contract obligations, evidence freshness, unresolved findings, incident history, monitoring results, and exit readiness.

8. Vendor Exit Checklist

- Disable accounts, API keys, plugins, and integrations.
- Export required logs, decision records, and evidence.
- Confirm data deletion, including retained prompts/outputs/backups where contractually covered.
- Remove vendor from authorized subprocessors/data-flow maps.
- Close inventory lifecycle status as Retired.
- Confirm alternative workflow and business continuity.
- Document outstanding disputes, incidents, or retained legal records.

Portfolio deliverable result

This standard turns procurement into a governance control: BrightBridge screens AI before purchase, obtains evidence, imposes child/data safeguards contractually, and maintains reassessment and exit discipline throughout the vendor lifecycle.