

AI Governance Charter & Operating Model

Enterprise decision rights, accountability, escalation, and governance cadence

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 Scope

BrightBridge Learning International is modeled as a International Children's Education Nonprofit with a 14-country simulated operating footprint, approximately 85,000 children and youth served annually, and approximately 1,650 employees and 3,200 volunteers. This Charter establishes how AI-related decisions are owned, reviewed, approved, monitored, escalated, and evidenced across the enterprise.

Charter objective

Ensure that AI use is purposeful, proportionate, child-centered, accountable, and supported by evidence before deployment and throughout the system lifecycle.

In Scope

- Internally developed AI/ML models and analytics that influence decisions.
- Generative AI tools used for learning, administration, communications, or analysis.
- AI-enabled features embedded within third-party SaaS products.
- Pilots, proofs of concept, research prototypes, and production systems.
- AI systems that are child-facing, child-affecting, employee-facing, donor-facing, or operational.

Out of Scope

- Conventional deterministic software with no adaptive, predictive, generative, or model-based functionality.
- Personal employee use of consumer AI tools is not authorized outside the separate acceptable-use rules and must never be used with BrightBridge restricted data.

2. Governance Principles

Principle	BrightBridge Standard
Child Safety First	Where AI affects children, safety and safeguarding take priority over speed, convenience, or optimization.
Human Accountability	AI may support decisions, but accountable human owners remain responsible for outcomes.
Privacy & Data Minimization	Collect and use only data necessary for the approved purpose, with heightened controls for child and safeguarding data.
Fairness & Inclusion	Assess bias, accessibility, local context, and differential impact before and after deployment.
Transparency & Explainability	Document purpose, limitations, responsible owners, affected stakeholders, and decision logic at a level appropriate to risk.
Evidence Before Conclusions	Approvals and risk acceptance require documented testing, controls, and evidence rather than assurances alone.
Proportionality	Governance depth increases with potential harm, vulnerable populations, automation, and uncertainty.
Continuous Monitoring	Approval is not permanent. Material changes, incidents, drift, or new evidence can trigger reassessment.

3. Governance Structure

BrightBridge uses a three-layer operating model: executive accountability, cross-functional governance, and system-level execution. Independent assurance provides challenge to the operating model and control effectiveness.

Layer	Primary Responsibility
Board / Executive Leadership	Sets risk appetite; receives quarterly material-risk reporting; reviews critical incidents and unresolved high residual risk.

Layer	Primary Responsibility
AI Governance Committee	Cross-functional approval and challenge body for high-risk AI, exceptions, material changes, and enterprise standards.
AI Governance Lead	Maintains inventory, classification, assessment workflow, committee materials, control/evidence tracking, and reporting.
System Owner + Control Owners	Operate the system within approved conditions; maintain controls, evidence, monitoring, and remediation.
Independent Assurance	Performs risk-based review of governance process and selected high-risk controls.

4. Named Roles and Responsibilities

Role	Illustrative BrightBridge Owner	Accountability
Executive Sponsor	Chief Executive Officer	Owns organizational AI risk appetite; resolves enterprise-level decisions; sponsors resources and board reporting.
AI Governance Chair	Chief Operating Officer	Chairs AI Governance Committee; owns operating model and cross-functional decisions.
AI Governance Lead	Director, Risk & Responsible Technology	Runs intake, inventory, assessments, committee materials, control tracking, and reporting.
AI System Owner	Named business executive for each system	Accountable for intended use, business value, risk treatment, controls, and lifecycle decisions.
Global Safeguarding Director	Child Safeguarding	Owns child-safety requirements, safeguarding thresholds, escalation criteria, and review of child-affecting AI.
Data Protection Lead	Data Protection Officer	Owns privacy review, data minimization, cross-border data considerations, retention, and privacy evidence.
Chief Information Security Officer	Information Security	Owns security controls, access, logging, incident coordination, and security due diligence.
Procurement/Vendor Risk Lead	Strategic Sourcing	Owns AI vendor intake, contract requirements, evidence collection, reassessment, and exit planning.
Regional Program Lead	Country/Regional Operations	Validates local context, implementation feasibility, human oversight, and community impact.
Internal Audit / Assurance	Independent assurance function	Performs risk-based assurance over governance process and control effectiveness.

5. Decision Rights

Decision	Recommends	Approves	Consulted	Rule
Register low-risk internal drafting tool	AI Governance Lead	System Owner	DPO / CISO as needed	Automatic only after intake completeness
Approve moderate-risk system	AI Governance Lead	Business Executive	Relevant control owners	May impose conditions
Approve high-risk child-affecting system	AI Governance Committee	Executive Sponsor	Safeguarding, DPO, CISO, Regional Program Lead	Formal decision record required
Accept High residual risk	Executive Sponsor	AI Governance Committee	Safeguarding / DPO / Legal as relevant	Board notification if material
Suspend system after critical incident	Global Safeguarding Director or CISO within domain	AI Governance Chair	System Owner	Immediate temporary suspension permitted
Approve exception to mandatory control	AI Governance Committee	Executive Sponsor	Control owner + Risk	Time-bound, documented compensating control required

Decision	Recommends	Approves	Consulted	Rule
Retire AI system	System Owner	AI Governance Lead	DPO, Procurement, CISO	Requires deletion/archival and vendor exit evidence

6. Governance Lifecycle

1. Business sponsor submits AI intake before purchase, pilot, or activation of an AI-enabled vendor feature.
2. AI Governance Lead creates or updates the inventory record and performs initial risk classification.
3. Required reviews are triggered by tier: safeguarding, privacy, security, fairness, accessibility, vendor, and legal/compliance as appropriate.
4. System Owner closes required controls and provides evidence.
5. Approval authority records Go, Conditional Go, Redesign, or No-Go.
6. System enters monitoring with defined KRIs, review cadence, and change triggers.
7. Material incidents, drift, new countries, model changes, new data uses, or purpose changes trigger reassessment.
8. Retirement includes access removal, data handling, contract exit, model/archive decisions, and closure evidence.

7. Escalation and Exception Process

Escalation Level	Trigger	Decision Body	Expected Action
Level 1 - Operational	Control gap or minor performance issue within approved tolerance	System Owner + AI Governance Lead	Corrective action tracked; no executive escalation unless overdue
Level 2 - Material	KRI breach, repeated fairness issue, privacy concern, or model performance below approved threshold	AI Governance Committee	Conditional operation, additional controls, or temporary restriction
Level 3 - Critical	Child safeguarding event, sensitive data exposure, prohibited-use concern, severe discrimination, or uncontrolled vendor change	Safeguarding/CISO/DPO + Executive Sponsor	Immediate containment or suspension; executive notification; documented incident review
Level 4 - Enterprise	Material unresolved residual risk, systemic control failure, or board-level risk appetite breach	Executive Sponsor / Board	No-Go, program pause, or enterprise remediation

Exception Requirements

- No exception may authorize a BrightBridge-prohibited AI use.
- Exceptions must identify the unmet control, rationale, duration, compensating control, accountable executive, residual risk, and expiry date.
- High-risk exceptions require AI Governance Committee approval and monthly review until closure.
- Expired exceptions automatically suspend the associated approval unless renewed before expiry.

8. Governance Cadence and Reporting

Cadence	Forum	Agenda	Owner
Monthly	AI Governance Operations Review	New intake; control gaps; overdue actions; KRI breaches; incidents; vendor changes	AI Governance Lead + control owners
Quarterly	AI Governance Committee	High-risk portfolio; approvals; residual risks; incidents; risk acceptance; roadmap	AI Governance Committee
Quarterly	Executive / Board Risk View	Top material AI risks; child safeguarding exposure; incidents; KRI trends; unresolved high residual risks	Executive Sponsor
Annual	Governance Maturity Review	Charter, risk standard, inventory completeness, training, control effectiveness, vendor program	AI Governance Lead + Internal Audit
Event-driven	Material Change / Incident Review	Critical incident; model change; new	Relevant decision authority

Cadence	Forum	Agenda	Owner
		country; new purpose; new sensitive data use	

9. Minimum Governance Records

- AI intake and inventory record
- Risk classification and rationale
- Required impact/risk assessments
- Control and evidence record
- Approval / decision record
- Exceptions and compensating controls
- Monitoring dashboard and KRI history
- Incident and escalation records
- Vendor due diligence and contract evidence
- Retirement / deletion / exit record

10. Charter Approval and Review

This simulated Charter would be approved by the Executive Sponsor on recommendation of the AI Governance Committee and reviewed at least annually or after a material change in organizational risk appetite, regulation, operating model, or AI portfolio.

Portfolio deliverable result

The Charter converts Responsible AI principles into a concrete operating model with named accountability, decision rights, escalation paths, evidence requirements, and governance cadence.