EDA COLLEGE

EDUCATE I DEVELOP I ACHIEVE

Risk Management Policy[1]

Version Control/History

Policy Title	Risk Management Policy
Policy Reference	EDA-GOV-RM-01
Version	1.1
Approved by	Board of Governors
Date of Approval	April 2026
Review Date	August 2026
Approval Date (V1.1)	11 September 2026
Next Review Date	Annual review of risk appetite and policy operation; full policy review every two years
Policy Owner	Designated Governor for Risk and Compliance
Applies To	All staff, governors, students in defined roles, contractors and partners involved in the management of risk on behalf of EDA College

[1] *Strategic Risk Framework, Risk Appetite and Three Lines of Defence, aligned with the OfS Public Interest Governance Principles, ISO 31000:2018, the COSO ERM Framework and the CUC Higher Education Code of Governance*

Contents

1. Policy Statement

EDA College ("the College") recognises that effective risk management is essential to the achievement of its mission, the protection of its students, staff and other stakeholders, and the long-term sustainability of the institution. The College adopts a deliberate, structured and embedded approach to risk management, in which risk is not treated as an obstacle to be eliminated but as an inherent feature of decision-making to be understood, weighed and managed.

This Risk Management Policy sets out the strategic framework for the management of risk across the College. It defines the College's risk philosophy, risk appetite, governance, lines of defence, and the relationship between risk management and the College's wider strategy, planning and assurance arrangements. It operates alongside the College's Risk Assessment Policy (which sets out the operational process by which risks are identified, scored and controlled) and supports compliance with the Office for Students (OfS) Regulatory Framework, in particular condition E2 (management and governance) and the Public Interest Governance Principles.

2. Purpose

The purpose of this policy is to:

- Set out the College's overarching framework for the management of risk.
- Define the College's risk philosophy, risk appetite and risk culture.
- Establish a clear, three-lines-of-defence model with defined roles and responsibilities.
- Define how risk management is integrated with the College's strategy, business planning, performance management and assurance arrangements.
- Define the categories of risk addressed and the risk appetite for each.
- Define the reporting and escalation arrangements that connect operational risk activity to Board-level oversight.

3. Scope

This policy applies to all activities undertaken by, or on behalf of, EDA College, including academic delivery, student services, governance, business operations, partnerships, subcontracted provision, events, research and the use of College premises. It applies to all employees (including agency, casual and temporary workers), members of the Board and committees, students in defined governance or representative roles, contractors, consultants, partners and volunteers.

4. Legal, Regulatory and Sector Framework

- Office for Students Regulatory Framework, in particular conditions E1 (public interest governance), E2 (management and governance), B1–B7, A1, A2, C1–C3 and (where applicable) E6, and the Public Interest Governance Principles (in particular Principle II – Risk Management).
- Higher Education and Research Act 2017.
- Companies Act 2006 and the general duties of directors (sections 171–177).

- Health and Safety at Work etc. Act 1974 and the Management of Health and Safety at Work Regulations 1999.
- UK GDPR and the Data Protection Act 2018.
- Bribery Act 2010 and the Modern Slavery Act 2015.
- Counter-Terrorism and Security Act 2015 (Prevent duty) and related statutory guidance.
- Equality Act 2010 and the Public Sector Equality Duty.
- ISO 31000:2018 Risk Management – Guidelines.
- COSO Enterprise Risk Management – Integrating with Strategy and Performance (2017).
- Institute of Internal Auditors Three Lines Model (2020).
- CUC Higher Education Code of Governance.

5. Definitions

5.1 Risk

The effect of uncertainty on the achievement of the College's objectives. Risk may have a negative effect (threat) or a positive effect (opportunity).

5.2 Risk Management

Coordinated activities to direct and control the College with regard to risk, including risk identification, assessment, treatment, monitoring and review.

5.3 Risk Appetite

The amount and type of risk that the Board of Governors is willing to accept in pursuit of the College's strategic objectives.

5.4 Risk Tolerance

The acceptable variation around the level of risk appetite for individual risks or risk categories.

5.5 Risk Capacity

The maximum amount of risk the College could absorb without breaching its strategic, regulatory or financial obligations.

5.6 Risk Culture

The values, beliefs, knowledge, attitudes and understanding about risk shared by individuals and groups within the College.

5.7 Risk Owner

The named individual accountable for the management of a specific risk.

5.8 Strategic Risk Register

The Board-level register of principal risks to the College's strategic objectives, owned by the Board and reviewed regularly.

5.9 Operational Risk Register

Departmental and programme-level registers of risks affecting day-to-day operations and the achievement of local objectives.

5.10 Three Lines of Defence

A model of risk governance distinguishing risk ownership and management (first line), risk oversight and policy (second line), and independent assurance (third line).

6. Risk Management Principles

The College's approach is based on the principles of ISO 31000:2018:

Principle	Application
Integrated	Risk management is integrated into all College activities, governance and decision-making.
Structured and comprehensive	It is structured, systematic and applied consistently across the institution.
Customised	It is customised to the College's context, objectives and stakeholders.
Inclusive	It draws on the knowledge and views of relevant staff, students and partners.
Dynamic	It is responsive to changes in the internal and external environment.
Best available information	It is based on the best available data, evidence and expert judgement.
Human and cultural factors	It takes account of human and cultural factors that influence risk and decision-making.
Continual improvement	It is improved continually through learning, monitoring and review.

7. Risk Philosophy and Culture

EDA College believes that:

- Risk-taking is a necessary feature of higher education and of innovation; the goal of risk management is informed risk-taking, not risk avoidance.
- Risks should be considered openly and proportionately, with as much attention to opportunities as to threats.
- Risk ownership lies with those closest to the activity, supported by clear escalation routes.
- Bad news must travel as fast as good news; staff at all levels are encouraged to raise concerns without fear of reprisal, in line with the Whistleblowing Policy.
- Risk management adds value when it informs decisions and protects students, staff, partners and the College, not when it generates paperwork for its own sake.

The Board, the Senior Leadership Team and managers at all levels are responsible for shaping and reinforcing the College's risk culture, including by modelling open conversation about risk, recognising near-misses and lessons learned, and challenging short-term decisions that create disproportionate long-term exposure.

8. Risk Appetite Framework

The Board of Governors approves and reviews the College's risk appetite at least annually, in line with strategy and the external environment. The Board uses a five-level scale to articulate appetite by category:

Level	Description
Averse	The College will avoid this category of risk wherever possible. Activity will only proceed where the risk has been reduced to a very low level. Used for risks to life, child safety and serious regulatory breach.
Cautious	The College accepts only limited exposure, with strong controls and active monitoring. Used for areas where the College has limited tolerance for adverse outcomes.
Balanced	The College accepts a moderate level of risk where the activity is well managed and aligned with strategic objectives. Used for most operational and strategic risks.
Open	The College is prepared to accept higher levels of risk in pursuit of clear strategic benefit, with appropriate controls. Used in areas of innovation and selective growth.
Hungry	The College is prepared to invest in opportunities with significant uncertainty where the potential strategic benefit is high. Used selectively and only with explicit Board approval.

9. Indicative Risk Appetite by Category

The College's indicative risk appetite by major category is summarised below; specific risk appetite statements are maintained in the College's Strategic Risk Register and reviewed annually.

Category	Indicative Appetite	Rationale
Student safety, safeguarding and wellbeing	**Averse**	The College has very low tolerance for risks to student safety, including safeguarding, sexual misconduct (OfS condition E6), Prevent and serious health and safety risks.
Regulatory and compliance (OfS, awarding bodies, PSRBs, UKVI)	**Averse**	The College has very low tolerance for breach of regulatory or sponsor duties.
Academic standards and student outcomes	**Cautious**	The College manages standards and outcomes risk tightly, with limited tolerance for adverse outcomes against B3 baselines.
Financial sustainability	**Cautious**	The College manages financial sustainability risk closely, in line with the Financial Regulations.
Information security and data protection	**Cautious**	Tight controls expected; tolerance for low-impact incidents but not for serious breaches.
Reputational risk	**Cautious**	The College is mindful of its reputation and exercises caution in decisions that could materially affect public confidence.
Operational risk	**Balanced**	Day-to-day operational risk is managed at programme and department level within agreed controls.
Curriculum innovation	**Open**	The College welcomes informed innovation in curriculum

and pedagogical experimentation		design and pedagogy, with appropriate evaluation.
Strategic partnerships and new markets	**Open**	The College is prepared to take measured risk on partnerships and growth, with strong due diligence and Board oversight.
Investment in major new initiatives (e.g. digital transformation)	**Hungry (selectively)**	Where the strategic benefit is significant and the case is robust, the Board will accept higher uncertainty.

10. The Three Lines of Defence Model

The College adopts the Institute of Internal Auditors Three Lines Model to clarify roles and responsibilities for risk management:

Line	Function	Examples at EDA College
First Line	**Risk ownership and management**	Heads of School / Programme Leaders, Heads of Department, line managers and staff who own activities and the risks attached to them. They identify, assess and manage risks day-to-day, supported by departmental risk registers.
Second Line	**Risk oversight, advice and policy**	The Designated Governor for Risk and Compliance, the Health and Safety Lead, the Data Protection Officer, the Safeguarding Lead and other specialist functions who set frameworks, provide advice, monitor compliance and challenge the first line.
Third Line	**Independent assurance**	Internal audit (commissioned through the Risk and Compliance Board), external audit and (where applicable) independent reviewers commissioned by the Board.
Governing Body / External Regulator	**Oversight and accountability**	The Board of Governors and the Risk and Compliance Board provide internal oversight; external regulators (e.g. OfS, awarding bodies, ICO, HSE) provide external accountability.

11. Risk Governance

Body / Role	Risk Responsibilities
Board of Governors	Approves the Risk Management Policy and risk appetite; owns the Strategic Risk Register; reviews principal risks at each Board meeting; ensures sufficient resources are in place; embeds risk in strategic decisions.
Risk and Compliance Board	Provides independent oversight of the operation of the risk management framework; reviews the Strategic Risk Register and assurance reports; commissions internal audit; receives reports on whistleblowing, fraud and major incidents.
Principal / CEO	Holds executive accountability for the operation of the risk framework; is the Accountable Officer for OfS purposes.

Senior Leadership Team	Maintains the Strategic Risk Register; identifies emerging risks; ensures risks are managed within appetite; reports to the Board.
Designated Governor for Risk and Compliance	Owns this policy; coordinates the College-wide risk management framework; supports the Risk and Compliance Board and the Board; provides training and tools.
Specialist second-line functions	Health and Safety Lead, Data Protection Officer, Designated Safeguarding Lead, Information Security Officer, Quality Assurance Lead, Director of Estates and Sustainability – each provides oversight, policy, advice and assurance in their domain.
Heads of School / Department / Programme Leaders	Identify, assess, control and monitor risks within their area; maintain operational risk registers; report incidents and significant new risks promptly.
All Staff and Students (in defined roles)	Cooperate with risk arrangements; follow agreed control measures; report hazards, incidents, near-misses and emerging risks; complete required training.

12. Strategic Risk Register

The Strategic Risk Register is the Board-level register of the College's principal risks. It contains, for each principal risk:

- A clear description of the risk and the strategic objective it threatens or supports.
- The risk owner (a named member of the Senior Leadership Team).
- An assessment of inherent likelihood and impact, residual likelihood and impact, and risk rating, using the 5×5 scoring methodology set out in the Risk Assessment Policy.
- A summary of existing controls and their effectiveness.
- Additional actions, owners and target dates to bring residual risk into appetite.
- Indicators that the risk is changing (e.g. KRIs).
- The relationship to OfS conditions of registration and other regulatory duties.

The Strategic Risk Register is reviewed quarterly by the Senior Leadership Team and the Risk and Compliance Board, and at each Board meeting. A deep dive on at least one principal risk is conducted at each Board meeting.

13. Operational and Project Risk

Operational and project risks are managed through registers maintained at programme, department or project level, in line with the Risk Assessment Policy. Each register:

- Is owned by a named risk owner with appropriate seniority for the area.
- Uses the College's standard 5×5 scoring methodology and risk language.
- Is reviewed at least quarterly, and following any significant incident or change.
- Feeds into the Strategic Risk Register where risks meet defined escalation thresholds.

14. Integration with Strategy, Planning and Performance

Risk management is integrated with the College's strategy, planning and performance arrangements through:

- Risk consideration in the development and review of the College's strategic plan and major programmes.
- Inclusion of risk and assurance information in business cases for major initiatives, capital expenditure and partnerships.
- Integration of risk reporting with financial and performance reporting to the Senior Leadership Team and the Board.
- Use of Key Risk Indicators (KRIs) alongside Key Performance Indicators (KPIs).
- Risk consideration in budget setting and resource allocation decisions.

15. Reporting and Escalation

Risk reporting follows clear lines from the operational level to the Board:

Audience	Reporting Frequency	Content
Heads of Department / Line Managers	Continuous	Departmental risk register; incidents and near-misses; emerging risks.
Senior Leadership Team	Monthly / Quarterly	Strategic and operational risk overview; emerging risks; key incidents; KRI dashboards.
Risk and Compliance Board	Quarterly	Strategic Risk Register; assurance reports; internal and external audit; whistleblowing summary; major incidents.
Board of Governors	Each scheduled meeting (at least four times a year)	Strategic Risk Register; principal risk deep dive; chairs' reports from committees; risk appetite review.
External regulators (OfS, awarding bodies, ICO, HSE, etc.)	As required	Statutory and regulatory notifications, including under PIGP XII (provision of information to OfS).

Risks that move outside the agreed appetite, or that breach defined escalation thresholds, are escalated immediately to the Senior Leadership Team and (where appropriate) the Risk and Compliance Board or the Chair of the Board.

16. Linkage with Related Arrangements

The risk management framework operates in close interaction with:

- The Risk Assessment Policy, which sets out the operational process for identifying, scoring and treating risks.
- The Internal Control Framework, including financial regulations, scheme of delegation and authority limits.
- Internal and external audit programmes.
- Health and safety risk assessments under the Health and Safety Policy and the Manual Handling Policy.
- Data Protection Impact Assessments (DPIAs) and information security risk reviews.
- Business Continuity, Critical Incident and Disaster Recovery arrangements.
- Anti-bribery, fraud, modern slavery, conflict-of-interest and whistleblowing arrangements.
- Academic governance and quality assurance arrangements (Academic Board).
- Safeguarding, Prevent, OfS condition E6 and student protection arrangements.

17. Emerging and Horizon Risks

The Board and Senior Leadership Team will give particular attention to emerging and horizon risks, including:

- Changes to the OfS Regulatory Framework and other higher education regulation.
- Demographic, market and competitor trends affecting recruitment and outcomes.
- Technological change, including the impact of artificial intelligence on teaching, learning and assessment.
- Cyber security threats and the evolution of the data protection landscape.
- Climate-related risks and the College's pathway to net zero.
- Geopolitical, economic and immigration developments affecting international students and staff.
- Sector-wide events such as the actions of the OfS, awarding bodies and PSRBs.

Horizon scanning is a standing item in the work of the Senior Leadership Team and the Board, supported by external scanning by the Designated Governor for Risk and Compliance.

18. Assurance Mapping

The College maintains an Assurance Map that links each principal risk to the sources of assurance available to the Board, distinguishing between first-, second- and third-line assurance. The Assurance Map informs the internal audit plan, the work of specialist second-line functions and the Board's view of where additional assurance may be needed.

19. Training and Capability

The College will provide proportionate training and capability development on risk management:

- Induction for Board members and senior staff covers the College's risk framework, risk appetite and the Three Lines model.
- Targeted training is provided for risk owners, second-line specialists and managers leading on major projects or partnerships.
- Refresher briefings are provided in response to significant changes in the regulatory environment, sector practice or the College's risk profile.
- Risk language and the 5×5 scoring methodology are embedded in standard project, partnership and procurement templates.

20. Records, Data Protection and Confidentiality

Risk registers, assurance reports, incident records and supporting documentation are maintained in line with the College's Records Retention Schedule. Personal data captured in incidents and risk events is processed in accordance with the UK GDPR, the Data Protection Act 2018 and the College's Data Protection Policy. Aggregate risk data is shared with the Board, regulators and (in anonymised form) with the wider sector where appropriate.

21. Roles and Responsibilities (Summary)

Role	Key Responsibilities
Board of Governors	Approves this policy; sets risk appetite; owns the Strategic Risk

	Register; reviews principal risks at each meeting.
Risk and Compliance Board	Provides independent oversight of risk management arrangements; reviews assurance and audit findings; reports to the Board.
Principal / CEO	Holds executive accountability for the operation of the risk framework.
Senior Leadership Team	Maintains the Strategic Risk Register; identifies emerging risks; ensures risks are managed within appetite.
Designated Governor for Risk and Compliance	Owns this policy; coordinates the College-wide framework; supports the Risk and Compliance Board and the Board.
Specialist Second-Line Functions	Provide oversight, policy, advice and challenge in their domains (H&S, data, safeguarding, IS, quality, sustainability).
Heads of School / Department / Programme Leaders	Identify, assess, control and monitor risks within their area; maintain operational registers; escalate as required.
All Staff	Cooperate with risk arrangements; follow controls; report incidents and emerging risks; complete training.

22. Monitoring, Reporting and Review

The implementation of this policy will be monitored through:

- Quarterly reviews of the Strategic Risk Register by the Senior Leadership Team and the Risk and Compliance Board.
- Annual review of risk appetite and the operation of the framework by the Board.
- Internal audit reviews of risk management arrangements and the operation of the Three Lines of Defence.
- External audit and (where appropriate) independent reviews of risk and governance arrangements.
- Aggregate analysis of incidents, near-misses, audit findings and whistleblowing concerns.

This policy will be reviewed at least every two years, or sooner where regulation, OfS conditions, sector guidance or the College's strategic environment require it.

23. Related Policies and Documents

- Risk Assessment Policy (operational scoring and process)
- Governance Framework and Board Standing Orders
- Financial Regulations
- Governance Framework with Terms of Reference
- Internal Audit Charter (where in place)
- Anti-Bribery and Corruption Policy
- Conflicts of Interest Policy
- Whistleblowing Policy
- Modern Slavery and Human Trafficking Statement
- Health and Safety Policy
- Data Protection Policy and DPIA Procedure
- Information Security Policy
- Safeguarding and Prevent Policy

- Bullying and Harassment Policy
- Business Continuity and Critical Incident Plan
- Student Protection Plan
- Academic Quality Assurance Policy
- Environmental and Sustainability Policy

24. Policy Approval

This policy has been approved by the Board of Governors of EDA College. It forms part of the College's suite of governance and compliance documents and will be communicated to all staff via induction and the staff intranet, and made available to students, partners and the public via the College website.

25. Version History

Version	Date	Author / Reviewer	Summary of Changes
1.0	April 2026	Designated Governor for Risk and Compliance / Risk and Compliance Board	First issue, aligned with the OfS Public Interest Governance Principles, ISO 31000:2018, the COSO ERM framework, the Three Lines Model and the CUC Higher Education Code of Governance.
1.1	September 2026	Designated Governor for Risk and Compliance / Risk and Compliance Board	Committee names aligned with the Governance Framework version 2.0; the Board of Governors named throughout. Approved 11 September 2026.

End of Policy