School of Coding & AI

RISK MANAGEMENT POLICY

1. Introduction

1.1 Purpose

The purpose of this Risk Management Policy ("Policy") is to set out School of Coding & AI's ("SOC") objectives and strategy for risk management, and the arrangements it has adopted to enable it to manage its risks.

There is a degree of risk involved in all of SOC's activities. Understanding those risks and managing them appropriately is critical to SOC's success. Effective identification and management of risk protect SOC's teaching, people (staff, students and visitors), resources and reputation.

This Policy provides a systematic framework for identifying, assessing, reporting and proactively managing risk, which enhances SOC's ability to make better decisions, respond quickly and effectively to exploit opportunities.

The aim of this Policy is not to eliminate risk from SOC's activities, but rather to ensure that every effort is made to manage risk appropriately and in line with SOC's risk appetite. This Policy also defines roles and responsibilities in relation to risk management and the processes for reporting risk within SOC.

This policy is owned and overseen directly by SOC's Board of Directors and embedded throughout the organisation. It informs strategic developments and the day-to-day management of activity.

Good risk management is vital for SOC's success and minimises failure. It supports and ensures:

- regulatory compliance (including initial registration and continued good standing with the OfS),
- financial stability;
- student protection (e.g. quality management, partnership continuity);
- strategic decisions in relation to prioritisation and management of educational partnerships; and
- effective governance effectiveness

1.2 Scope

At an institutional level, risks may influence the organisation's capacity to operate effectively as a business, meet its regulatory obligations, and deliver its strategic and academic objectives. Effective risk management is therefore essential across all areas of activity, including academic delivery, professional services, and partnership operations, to ensure that threats and opportunities affecting the successful delivery of plans are identified, assessed, and managed appropriately.

This Policy applies throughout SOC to all staff, including the senior leadership team and Board of Directors.

1.3 Definition

For the purposes of this Policy, "risk" refers to the possibility that an action, event, or set of circumstances may affect SOC's ability to achieve its strategic objectives or damage its reputation. This impact may be negative (a threat) or positive (an opportunity).

2. Risk Management Principles

- Integrated: Risk management considerations are embedded in strategy, day to day operations, and decision-making (Board reserved matters).
- Proactive & Proportionate: risks are managed proactively in an effective and efficient manner with proportionate processes and procedures recognising that changes in risk profile can affect more quickly and deeply a specialist higher education provider.
- Three Lines of Defence:
    - Operational owners (daily management).
    - Oversight (Principal, committees).
    - Assurance (quality reviews by partners or PSRBs, external review).
- Accountability: accountability for risk is clearly defined as set out in section 3 of this Policy;
- Transparent: risk management is transparent across SOC activities with timely reporting and clear escalation lines to enable informed governance;
- Monitoring: continuous improvement in risk management is achieved through continuous monitoring, review and accurate record keeping.

3. Roles and Responsibilities

Role	Key Responsibilities
Board of Directors	- Approve this Policy, the Risk Appetite Statement, and review the Corporate Risk Register at each meeting. - Ensure alignment with student protection plan, business plans and financial forecasts. - Review the Corporate Risk Register at each meeting and gain assurance on controls and mitigation plans.
Principal and (Accountable Officer)	- Own the Corporate Risk Register; escalate high risks or changes in risk profile to the Board. - Embed risk in operational decisions (including provisions in the Schedule of Delegation). - Report to OfS on reportable events.
Academic Board	- Own academic/quality risks (including those relating to student satisfaction and students' outcomes: continuation, completion, progression). - Monitor partner delivery in collaborative teaching arrangements.
Clerk to the Board	- Record risk discussions in minutes of meetings. - Maintain the Corporate Risk Register and report trends.
Senior Management Team	- Identify/own divisional or departmental risks; implement mitigations. - Conduct monthly reviews as part of Senior Management Team meetings.
All Staff/Partners	- Responsibility for identifying, evaluating and managing risk within their area of responsibility. - Assist with the implementation of risk mitigation strategies relevant to their role; and - Report risks via escalation channels.

4. Risk Appetite Statement

Risk appetite is the level and type of risk the SOC is willing to accept in pursuit of its strategic objectives. In particular, it expresses how much uncertainty SOC is prepared to tolerate in different areas of operations. The Board of Director's tolerance for risks is set out below and is reviewed annually:

Category	Appetite	Tolerance	Escalation Trigger
Student Outcomes	Very Low	B conditions - absolute thresholds need to be met	Any variance → Principal immediate
Regulatory (OfS)	Very Low	Zero reportable events	Any breach → Board of Directors
Financial	Low	≥3 months reserves	Forecast breach → Principal
Partnerships	Moderate	≥1 active partner; 90% revenue	Termination risk → Principal
Operational	Moderate	No major incidents/year	Medium → Relevant Senior Management Team lead and/or committee
Reputational	Low	No negative media escalation	High impact → Board of Directors

5. Risk Assessment and Reporting

5.1 Risk Assessment

SOC's assessment and scoring of risk are based on a 9-point scale, as follows:

Impact (A–C)

- **A – Major impact:** significant financial, operational, legal, or reputational consequences.
- **B – Moderate impact:** affecting the whole organisation to a lesser extent, or significantly impacting the operation, reputation or strategic direction of part of the organisation.
- **C – Minor impact:** some impact on part of the organisation and/or includes a financial impact relating to a project or initiative over one or multiple years.

Likelihood (1–3)

- **1 – Almost certain** within 1-2 years
- **2 – Possible/likely** within 2+ years
- **3 – Unlikely**

Risk Matrix:

	Likelihood 1 (Almost Certain)	Likelihood 2 (Possible/Likely)	Likelihood 3 (Unlikely)
A (Major)	High (A1)	High (A2)	Medium (A3)
B (Moderate)	High (B1)	Medium (B2)	Low (B3)
C (Minor)	Medium (C1)	Low (C2)	Low (C3)

Ratings: High = Immediate escalation; Medium = Board review; Low = Monitor.

The above risk scoring matrix has been designed explicitly as a tool, supporting clear decision-making and more effective oversight:

- Clarity and Communication: Letter–number combinations (e.g., A1) are easier to interpret at a glance than abstract scores like 12 or 16. Solely numerical ratings can also give a spurious sense of accuracy that is often not possible when assessing risk.
- Encourages Structured Risk Conversations because the system forces discussion around two separate dimensions: i.e. what can be managed either to mitigate the impact (sometimes more within the scope of influence for the organisation) and/or the likelihood of the risk happening.

5.2 Risk Management Process

1. Identify: risks are identified through monthly team meetings, partner feedback, OfS-related data, and monitoring changes in the external environment.
2. Assess: each risk is assessed and scored by the risk owner, and the Principal validates the risk ratings.
3. Mitigate: mitigation actions are assigned to risk owners with agreed deadlines. Progress against such actions is reviewed at the monthly senior management team meeting.
4. Reporting and assurance: reporting and assurance activities are carried out in accordance with the arrangements set in section 6 of this Policy.

5.3 Corporate Risk Register

A corporate risk register is a structured means of identifying and classifying risk in a consistent and coherent manner, and for assigning risk ownership. It also documents existing controls, the current and target status of each risk and further actions being taken to mitigate risk.

SOC's Corporate Risk Register has the following fields:

- **Risk ID**: alphanumerical identifier
- **Risk description**: explaining the cause/trigger (in the external environment) and describing the impact, e.g. in terms of student numbers or outcomes, financial implication, reputational damage.
- **Risk Owner:** relevant members of SMT
- **Gross risk rating:** Initial rating of a risk without any controls or responses.
- **Controls:** existing actions or mechanisms in place to mitigate the likelihood and/or impact of the risk happening, based on the four Ts of risk management:
  - Tolerate: Accept the risk because it is low or the cost of reducing it would be higher than the potential impact.
  - Treat: Take action to reduce the likelihood or impact of the risk (for example, extra controls, procedures, or training).

- Transfer: Shift some or all the financial or practical consequences to another party (for example, insurance or contractual arrangements).
- Terminate: Remove the risk entirely by stopping, redesigning, or not undertaking the activity that creates it.

- **Net risk rating:** based on the application of existing controls specified.
- **Planned actions** (including action owners, deliverables and deadlines): to develop further controls that may lower further the net risk rating.

6. Reporting and Assurance

- Monthly: Principal review of risk with senior management team.
- Each meeting: Board paper (full Corporate Risk Register, risk appetite compliance update).
- Annual: review of governance statement (Annual Report/OfS return).

This Policy is reviewed annually by the Board of Directors.

7. Training and Resources

- All relevant staff and directors receive annual risk awareness briefings.

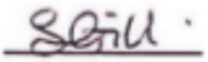
8. Related Policies

- Schedule of Delegation (Code of Governance, Annex C),
- Student Protection Plan
- Anti-Bribery and Counter Fraud Policy

9. Further Information

For further information, please contact the Clerk to the Board at clerk@schoolofcoding.co.uk

Name of provider: School of Coding & AI Ltd
Name of nominated accountable officer: Suki Gill
Designation: Principal

Signature: 
Date: 18th June 2026