REDHILL ACADEMY TRUST

Equality and Achievement

Risk Management Policy

APPROVING BODY	AUDIT AND RISK COMMITTEE
DATE APPROVED	JULY 2026
VERSION	2.0
SUPERSEDES VERSION	N/A
REVIEW DATE	JULY 2027
FURTHER INFORMATION / GUIDANCE	• Academy Trust Handbook • DfE guidance – Academy trust risk management

CONTENTS

1 – PURPOSE AND SCOPE

This policy outlines the framework for identifying, assessing, managing, and monitoring risks across Redhill Academy Trust. It ensures that risk management is embedded in all levels of decision-making to protect the Trust's assets, reputation, and ability to deliver high-quality education.

This policy applies to:

- All academies within the Trust
- Trustees, Local Governing Bodies, Executive Leaders, and Staff
- All operational, financial, strategic, compliance, and reputational risks

Definitions

- Executive Trust Board of Directors to also mean Board of Trustees
- Chief Executive Officer to also mean Accounting Officer

2 - ORGANISATION OF RESPONSIBILITY & ACCOUNTABILITY

The Trustees delegate the day-to-day responsibility of managing and implementing the Risk Management policy to the Chief Executive Officer to ensure risks are managed in accordance with this policy.

3 - OBJECTIVES

- Promote a culture of proactive risk management
- Ensure risks are identified, assessed, and mitigated effectively
- Support strategic planning and operational delivery
- Comply with legal, regulatory, and funding requirements
- Safeguard pupils, staff, and stakeholders

4 – ROLES AND RESPONSIBILITIES

Trust Executive Board: Overall accountability for risk management and reviews the Trust Risk Registers.

Audit & Risk Committee: Monitors risk management processes; approves the Risk Management Policy, reviews key risks and mitigation strategies.

CEO & Executive Team: Implements the policy; maintains the Trust Risk Register; ensures risk awareness across the Trust.

Headteachers: Identify and manage risks at academy level; maintain local risk registers.

All Staff: Report risks and follow risk mitigation procedures.

5 – RISK MANAGEMENT PROCESS

5.1 Identification

Risks are identified through strategic planning, operational reviews, incident reporting, and audits.

5.2 Assessment

Each risk is assessed based on Likelihood (1–5) and Impact (1–5). Risk Score = (Likelihood × Impact) + Impact. Each risk is assigned a status as below:

RATING	IMPACT
1	Negligible
2	Minor
3	Moderate
4	Major
5	Serious

RATING	LIKELIHOOD
1	Rare (below 10%)
2	Unlikely (11-40%)
3	In the balance (41-60%)
4	Likely (61-90%)
5	Almost certain (above 90%)

RATING	STATUS
D	Declining
S	Stable
I	Increasing
N	New

5.3 Mitigation

Mitigation strategies include avoidance, reduction, transfer (e.g., insurance), and acceptance (with monitoring).

5.4 Monitoring and Review

Risk registers are reviewed termly and updated as needed. Significant risks are escalated to the Executive Board. Trends in risk exposure are tracked over time and reported to the Audit & Risk Committee.

6 – RISK CATEGORIES

- Education: Political, environmental, demographic, reputation, long-term planning
- Operational: Staffing, IT systems, safeguarding, legal, regulatory, data protection, governance
- Financial: Budgeting, fraud, funding

7 – RISK APPETITE

The Trust adopts a balanced risk appetite:

- Low tolerance for safeguarding, compliance, and financial mismanagement
- Moderate tolerance for innovation and educational improvement initiatives

8 – FOUR LINES OF DEFENCE

1. Operational Management: Own and manage risks

2. Risk Oversight: Risk and compliance functions

3. Internal Scrutiny: Independent assurance (e.g. internal audit)

4. External Assurance: External audit and regulatory review

The Audit and Risk Committee directs the internal scrutiny programme. This includes setting the scope, frequency, and focus areas of internal audits. Findings are reported to the Executive Board with action plans and follow-up reviews to ensure continuous improvement.

9 – RISK CONTROL STRATEGIES

The Trust adopts the 5 'T's approach to risk control strategy.

- **Tolerating** risk is where no action is taken. This may be because the cost of instituting controls is not cost-effective, or the risk or impact is so low that they are considered acceptable.
- **Treating** risk involves controlling it with actions to minimise the likelihood of occurrence or impact. There may also be contingency measures to reduce impact if it does occur.
- **Transferring** risk may involve the use of insurance or payment to third parties willing to take on the risk themselves (for instance, through outsourcing).
- **Terminating** risk can be done by altering an inherently risky process to remove the risk. If this can be done without materially affecting operations, then removal should be considered, rather than attempting to treat, tolerate or transfer.
- **Take advantage** of a risk in recognition that the uncertainty attached to risk sometimes offers opportunities as well as threats.

10 – CONTINGENCY AND BUSINESS CONTINUITY PLANNING

The Trust maintains contingency and business continuity plans to ensure resilience and recovery in the event of disruption.

11 - REVIEW

This policy is reviewed and approved annually by the Audit & Risk Committee.