Risk and Issue Management Policy

2026/2027 Academic Year

Contents

---

1. Aims

Our trust aims to:

- Set out the framework our trust has adopted for risk management
- Identify, measure, manage, monitor and report threats to the trust's business objectives
- Embed risk management processes in both day-to-day operations and governance

2. Legislation

This policy is based on the following statutory and non-statutory guidance from the Department for Education (DfE):

- Academy Trust Handbook
- Academy trust risk management

This policy also complies with our funding agreement and articles of association.

3. Definitions

3.1 Board of Trustees

The Board of Trustees (the Board) will:

- Take overall responsibility for risk management, including contingency and continuity planning
- Determine the risk appetite
- Appoint an audit and risk committee in accordance with the Academy Trust Handbook

3.2 Audit and risk committee

The Operations Committee will act as the audit and risk committee and will:

- Direct the trust's programme of internal scrutiny
- Ensure that risks are being addressed appropriately through internal scrutiny
- Have oversight of the risk register
- Report to the trust board on the adequacy of the trust's internal control framework, including financial and non-financial controls and management of risks

3.3

Local governors will:

- Work with the trust leadership team to identify risks and ensure plans are in place to minimise any impact on the academy trust and its pupils

3.4 Executive Headteacher

The Executive Headteacher will:

- Have prime responsibility for risk

3.5 Headteachers

Within their own academies, Headteachers will:

- Carry out day-to-day risk management
- Assess operational risks
- Identify and report risks to the Operations Committee

4. Risk identification

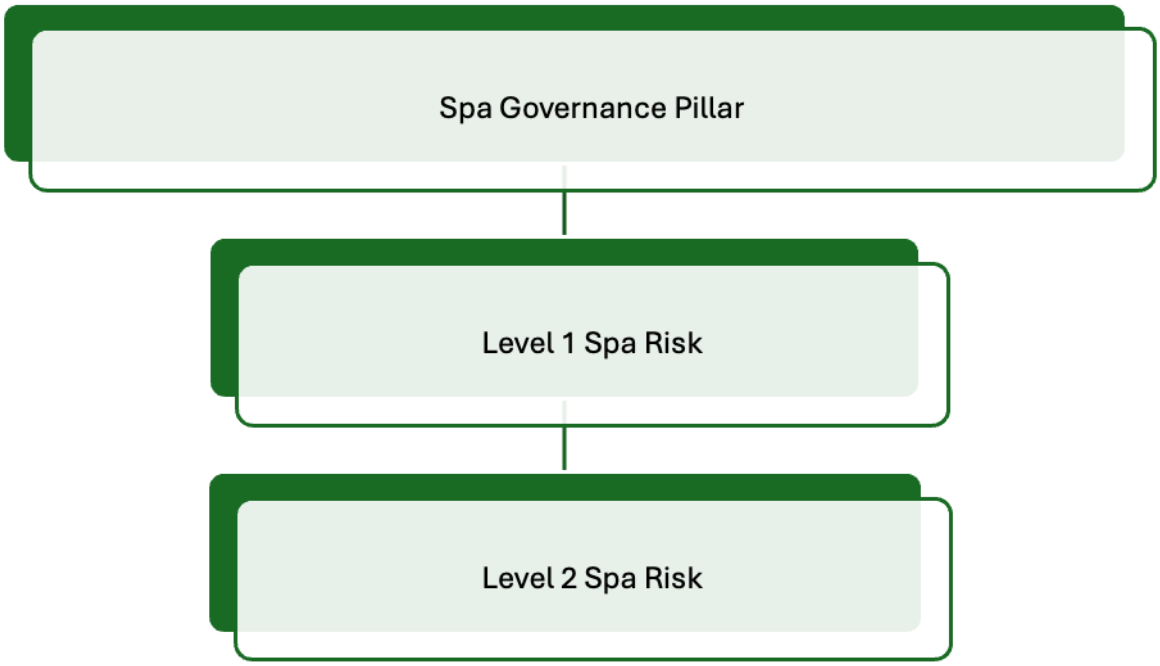
A risk is any potential event or threat (including not capitalising on opportunities) which could impact the Trust's ability to meet its objectives.

The Board takes a top-down approach to the identification and management of risks. The trust operates under five governance pillars:

1. Finance and Operations
2. School Improvement
3. Workforce
4. Safeguarding
5. Governance

At least one Trustee is assigned to each Governance pillar and oversees the work performed under the governance pillar at the Board level.

The trust's risk management framework follows a hierarchical approach to establish a link between the granular risks identified (Level 2 Spa Risk) and the governance pillar that is responsible for monitoring the risk and associated activities. Risks which are similar are grouped together under the same Level 1 Spa Risk. This approach allows the Operations Committee to better understand the ever-evolving risk profile of the trust.



The following Level 1 Spa Risks are utilised:

- Compliance
- Finance
- Procurement
- Technology
- Governance
- Strategy
- Education
- Environment
- People Management

At the risk identification stage, all potential events that are a threat to the achievement of business objectives (including not capitalising on opportunities) are identified, defined and categorised. These are considered Level 2 Risks and must be mapped according to the hierarchy to ensure that there is a link between the risk and the Board.

5. Risk assessment

Risk measurement consists of assessment, evaluation and ranking. This ensures all identified risks are compared according to a consistent standard.

5.1 Assessment

The aim of assessment is to better understand each specific instance of risk, and how it could affect business objectives. Risks are assessed based on:

- The likelihood (or probability) of it occurring, and
- The impact (or severity) if it did occur

Both of the above risk factors are assessed using a 5-point scale:

Descriptor	Score	Probability	Impact
Very High	5	Likely occurrence within a week	• Trust-wide impact affecting the ability to continue operations • Irreversible reputational damage • Financial loss equal to 50% or more of Trust income • Major breach of legal or regulatory requirements resulting in closure or prosecution • Loss of life or serious safeguarding failure
High	4	Likely occurrence within a month	• Multiple schools affected or prolonged service disruption • Sustained reputational damage • Financial loss between 25–49% of Trust income • Serious breach of policy, regulation or safeguarding requirements • Major staff or stakeholder dissatisfaction
Medium	3	Likely occurrence within a year	• Single school or department significantly affected • Local reputational damage requiring intervention • Financial loss between 10–24% of Trust income

			• Breach of internal policies or minor legal/regulatory breach • Staff morale or student outcomes impacted
Low	2	Likely occurrence within two years	• Temporary or localised impact on operations • Limited reputational concern manageable with internal communication • Financial loss between 5–9% of Trust income • Minor policy non-compliance • Minimal impact on staff, pupils, or outcomes
Very Low	1	The risk is unlikely to ever materialise.	• Negligible operational disruption • No reputational impact • Financial loss under 5% of Trust income • No breach of policy or regulation • No adverse impact on people or performance

A risk score can be calculated by multiplying together the likelihood and impact scores to arrive at the following RAG ratings:

		Impact				
		Very low	**Low**	**Medium**	**High**	**Very high**
Likelihood		**1**	**2**	**3**	**4**	**5**
Very high	**5**	5	10	15	20	25
High	**4**	4	8	12	16	20
Medium	**3**	3	6	9	12	15

		Impact				
Low	**2**	2	4	6	8	10
Very low	**1**	1	2	3	4	5

5.2 Inherent risk

Inherent risk refers to the level of risk that exists in the absence of any controls or mitigating actions. It captures the potential impact and likelihood of a risk materialising in a worst-case or control-absent scenario.

The 'inherent risk score' is calculated by multiplying the likelihood and impact risk scores together (determined on the basis that there is no treatment or controls applied to mitigate the risk) to derive a single inherent risk score reflecting its overall level of threat.

5.3 Residual risk

Residual risk is the level of risk that remains after controls, mitigations, and other risk treatments have been implemented (see section 6). It reflects the exposure that the trust continues to face, even after taking steps to manage or reduce the inherent risk.

The 'residual risk score' is calculated by multiplying the likelihood and impact risk scores together (determined on the basis that there are effective controls and/or other measures applied to mitigate the risk) to derive a single residual risk score.

6. Risk appetite

Risk appetite indicates the amount of risk the trust is willing to accept in the pursuit of its strategic objectives. As identified in the UK Code of Corporate Governance, risk appetite is set by the Board, in considering the trust's strategic goals and how these will be achieved. Hence, the trust has a range of appetites for different types of risks, dependent on how they may impact on the trust's objectives.

Four levels of risk appetite have been defined by the Board. Each of these appetite levels reflect a willingness to take on a different level of risk:

- Averse - Very safe approach with the avoidance of all but the minimum risks

- Cautious - Preference for safe, though accept there will be some low risk exposure
- Open - Open to considering potential options recognising that there will be risk exposure
- Willing - Willing to innovate and take risks.

The Board currently operates between a cautious and open risk appetite and therefore requires management to implement risk control measures (see section 7) to reduce the residual risk of all level 2 risks to below 10.

7. Risk control

The Board will consider the '4 Ts' when deciding the appropriate risk treatment option(s), balancing the potential benefits from the achievement of objectives against the costs, efforts, or disadvantages of proposed actions.

- **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.
- **Treat** 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.
- **Transfer** risk may involve the use of insurance or payment to third parties willing to take on the risk themselves (for instance, through outsourcing).
- **Terminate** 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 will be considered, rather than attempting to treat, tolerate or transfer. Alternatively, if a risk is ranked highly and the other potential control measures are too expensive or otherwise impractical, the rational decision may well be that this is a process the academy trust will not be performing at all.

7.1 Controls inventory

The trust maintains an inventory of its controls on the Risk Register and maps the controls back to the risks which they mitigate. This allows the Operations Committee to easily determine the impact of a control failure on the risk and determine whether the risk is being appropriately mitigated in line with the risk appetite set by the Board.

8. Incident identification

The Board recognises that even when risks are treated, they could still materialise and it is important that these incidents are properly recorded to ensure that:

- Leadership is aware of incidents which have occurred and can undertake remedial action as required;
- Lessons can be learned to prevent the risk from rematerialising;
- There are no unidentified risks;
- The Operations Committee can make an informed decision on the effectiveness of the measures put in place to manage the risks identified.

To achieve these objectives, the trust maintains an Events Register on the Risk Register. An event MUST be recorded to reflect:

- There is a breach or non-conformance with a Trust policy, regulation or legislation
- An operational error e.g. money incorrectly paid out of a Trust bank account
- Fraud
- A data protection breach (GDPR breach)
- Health and Safety event e.g. fall on site
- Activation of the Business Continuity Plan
- Break-in or security lapse
- Audit finding

The above list is not exhaustive and the Operations Committee encourages any potential event to be recorded. The Board has a zero-tolerance policy on retaliation against staff that raise concerns in good faith.

8.1 Event reporting

All events are assigned a unique identifier and the register will at all times show the status of the event as either open or closed. The following information will be captured:

Field	Guidance
Reporter	The name of the staff member that identified/reported the event or issue. In the case of audit findings, these will be recorded as “Internal Audit” or “External Audit”
Identified Date/ Start Date/ End Date	The date the issue was identified and an estimation of when the event started and ended.

Spa Risk	The Level 1 and Level 2 Spa Risks that the event relates to which must align to the hierarchy on the risk register.
Description	A detailed description of the events
Corrective Actions/Lessons Learned	A description of the actions that will be taken to remediate and prevent recurrence of the event.
Action Owner	The staff member responsible for implementing the actions.
Linked Event	Events which are linked
Approver	Each event must be approved for accuracy by an approver. The approver also confirms that the corrective action plan is appropriate and has been correctly implemented. Only Headteachers and above may act as event approvers.

8.2 Trustee oversight

All events are recorded against a Spa governance pillar and the Trustee responsible for that pillar must review all events recorded once per term and report to the Operations Committee any thematic issues, material concerns or other points of note.

9. Monitoring and reporting

Monitoring is ongoing and continuous, as this supports the trust's understanding of whether and how the risk profile is changing. Monitoring also provides assurance on the extent to which the mitigating actions and controls are operating as intended and whether risks are being managed to an acceptable level.

The risk register is central to risk monitoring. As risks are identified, they will be logged on the register and the associated control measures documented. For each identified risk, the Trust must record the data points which can be utilised to determine the impact and likelihood of the risk materialising.

The risk register will be updated by the Senior Leadership Team.

The risk register is a live document and is an ongoing process. The Board will undertake an annual high-level risk register annually.

The Operations Committee will review the risk register termly, which will also include assessments of effectiveness of controls and mitigating plans of major risks. The Board will keep the trust's risk appetite under review and consider the ongoing appropriateness of the risk management policy.

In the event of unforeseen circumstances, the Board will consider the extent to which the risk was identified and measured and whether the selected control measure was appropriate. The risk register will facilitate a rational risk-based approach for the internal scrutiny function's work programme. The audit and risk committee are responsible for directing the trust's programme of internal scrutiny, which will focus on:

- Evaluating the suitability of, and level of compliance with, financial and non-financial controls
- Offering advice and insight to the board on how to address weaknesses in financial and non-financial controls
- Ensuring all categories of risk are being adequately identified, reported and managed

10. Monitoring and review

The Operations Committee is responsible for the implementation of this policy. The policy will be reviewed and approved every year. The Board is responsible for determining the Trust's risk appetite.

11. Links to other policies and documents

- Risk Register
- Business Continuity Plan (BCP)