PROSPER TOGETHER
MULTI ACADEMY TRUST

RISK MANAGEMENT POLICY

APPROVED BY TRUSTEES

SIGNED...P. JACKSON……………………………………….

ROLE …CHAIR OF F.A & R. COMMITTE…………….

DATED …MAY 2023…………..………………………………

DATE	PREPARED BY	REVIEW DATE
MAY 2023	S Timmins	MAY 2024

1. Purpose

The purpose of this policy is to set out how Prosper Multi Academy Trust (the Trust) will identify and manage current and future risks to ensure it can further its charitable objects, protect its staff and assets and ensure financial sustainability.

The effective management of risk will inform the Trust's business decisions, enabling a more effective use of resources and ensuring there are robust strategic, business, and contingency planning activities in place.

2. Scope

This policy applies to the Trust and all member schools. The identification and monitoring of risk applies to all areas of the Trust's business.

3. Policy Statement

The Trust is committed to effectively identifying and assessing risks, evaluating the actions that are required to manage those risks and ensuring there is periodic monitoring and assessment.

Our aim is to ensure that:

- Significant strategic and operational risks are known and monitored, enabling informed decisions and timely action to be taken.
- Risks are identified and assessed at a formative stage as opportunities arise.
- The Trust's common purpose, vision, strategic priorities and operational plans are achieved successfully.

Our objectives are to:

- Protect the Trust's children, staff and assets.
- Manage risk in accordance with best practice and reduce the cost of risk.
- To anticipate and respond to changing social, environmental and legislative requirements.
- Raise awareness of the need for effective risk management.
- Integrate risk management into the culture of the Trust.
- Adopt legal compliance as a minimum standard.

These aims and objectives will be achieved by:

- Establishing and maintaining a risk management organisational structure to act in an advisory and guiding capacity which is accessible to all staff.
- Maintaining documented procedures for the control of risk.
- Providing suitable information and training to staff.
- Maintaining effective communication and the active involvement of all staff.
- Maintaining an appropriate incident reporting and recording system, with
- investigation procedures to establish cause and prevent recurrence.
- Monitoring arrangements on an ongoing basis.

4. Approach to Risk Management

Risk management can be considered in terms of the ICAEW (Institute of Chartered Accountants in England & Wales) four lines of defence model which is a concept for helping to identify and understand the different contributions various sources can provide:

- **1st line of defence** – management and staff who own and manage risk on a day-to-day basis.

- **2nd line of defence** – the board who oversee the effectiveness of the risk management framework.

- **3rd line of defence** - the internal scrutiny function who provide independent assurance on the overall effectiveness of risk management and controls.

- **4th line of defence** - assurance from external independent bodies such as the external auditors and other external bodies.

The Trust will ensure that risks are being addressed appropriately through internal scrutiny and will regularly assess the adequacy of the Trust's internal control framework, including financial and non-financial controls and management of risks.

5. Roles and Responsibilities

4.1 Trustees:

The Trust Board will review this policy and monitor its effectiveness to ensure risk is managed appropriately across the organisation. Trustees will determine the desired risk profile, approve major decisions which affect that profile and ensure the organisation learns from its response to risk. The Trust Board has overall responsibility for risk management including at least annual oversight of the Central risk register.

4.2 Finance, Audit and Risk Committee:

The committee oversees internal controls, internal assurance and external audit across the trust. It will monitor the implementation of this policy, ensure that risks are being addressed appropriately through internal scrutiny and report to the board on the adequacy of the trust's internal control framework, including financial and non-financial controls and management of risks.

4.3 Accounting Officer:

The Trust's accounting officer, who is the Chief Executive Officer (CEO), is accountable to the board for the management of opportunities and risks on behalf of the trust and ensuring agreed actions are implemented.

4.4 Headteachers and Local Governing Boards (LGBs):

The Headteacher and LGBs will be involved in identifying, assessing and managing risks relevant to their individual school. This should include:

- Identifying and evaluating the significant risks faced by their operations for consideration by the LGB and subsequently the Trust's Finance, Audit and Risk Committee.
- The LGB reviewing the school risk register termly.

- Reporting to the COFO each term any changes to the risk register and at the earliest opportunity when a significant risk is identified.
- Ensuring that risk management is incorporated at the conceptual stage of projects, as well as throughout a project.
- Ensuring that risk management is a regular management meeting item to allow consideration of exposure and to prioritise work in the light of effective risk analysis.
- Report early warning indicators to the Central Executive Team of the Trust.

4.5 Chief Operating and Financial Officer (COFO):

The COFO has responsibility for the organisation and implementation of the risk management process. This should include:

- Developing specific programmes and procedures for establishing and maintaining risk management activities within the Trust.
- Ensuring the dispersal of vital information.
- Providing guidance, interpretation and understanding of the risk management systems.
- Managing the overall, collective risks faced by the Trust.
- Risk management across the Trust on a day-to-day basis.

4.6 Risk owner:

This is the person who has responsibility for ensuring any actions identified to manage the risk are effectively implemented.

4.7 Staff:

All staff members are responsible for the effective management of risk within their area of activity and responsibility, including the identification of potential risks. Staff should be enabled to ‘speak up’ about any potential business or operational risk that they identify, including through related management policies and procedures (eg. Health and Safety, Fraud Prevention, Whistleblowing, Safeguarding).

6. Risk Identification and Recording (Risk register)

At the risk identification stage, all potential events that are a threat to the achievement of the Trust’s business objectives are identified, defined and categorised.

Risk is not only about adverse events, but also about missed opportunities.

All areas of activity within the Trust, its schools, and partnerships with third party organisations should be considered, together with what would stop them being as successful as they should. The key risks that the Trust and the schools face will be those that would stop the Trust or its schools achieving their objectives in these areas.

As the first step in the risk identification process, all staff with responsibility for delivering operations aims or targets need to understand the Trust’s and the legal and regulatory environment in which it operates.

The next step is to identify what would stop each area being as successful as it should.

Understanding the type of risk being faced can help to determine what action is best to take. Risks are grouped according to the following categories:

- **Strategic risks** – Risks arising from identifying and pursuing a strategy, which is poorly defined, is based on flawed or inaccurate data or fails to support the delivery of commitments, plans or objectives due to a changing macro-environment (e.g. political, economic, social, technological, environment and legislative change).

- **Governance risks** – Risks arising from unclear plans, priorities, authorities and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance.

- **Operations risks** – Risks arising from inadequate, poorly designed or ineffective/inefficient internal processes resulting in fraud, error, impaired customer service (quality and/or quantity of service), non-compliance and/or poor value for money.

- **Legal risks** – Risks arising from a defective transaction, a claim being made (including a defence to a claim or a counterclaim) or some other legal event occurring that results in a liability or other loss, or a failure to take appropriate measures to meet legal or regulatory requirements or to protect assets (for example, intellectual property).

- **Safety risks** – Risks arising from safety deficiencies or poorly designed or ineffective/inefficient hazard management resulting in non-compliance and/ or harm and suffering to pupils, staff, contractors, service users or the public.

- **Financial risks** – Risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting.

- **Commercial risks** – Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, and /or failure to meet business requirements/objectives.

- **People risks** – Risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviours, the unavailability of sufficient capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance.

- **Technology risks** – Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.

- **Information risks** – Risks arising from a failure to produce robust, suitable and appropriate data/information and to exploit data/information to its full potential.

- **Security risks** – Risks arising from a failure to prevent unauthorised and/or inappropriate access to the estate and information, including cyber security and non-compliance with General Data Protection Regulation requirements.

- **Project/Programme risks** – Risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost and quality.

- **Reputational risks** – Risks arising from adverse events, including ethical violations, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damages to reputation and or destruction of trust and relations.

The risks that have been identified should be recorded on the appropriate **risk register**, depending on whether the risk is identified by an individual school or the Trust.

At school-level, each school within the Trust should identify and thereafter record their risks in their school's risk register. The risks that have been identified at Trust-level should be updated to the Trust's Central Risk Register.

At board level, risk management assessment will focus on the highest priority risks, which will have the greatest impact on the Trust. School and executive leaders will need to assess operational risks. The role of the FAR Committee is to oversee that all categories of risk are identified and must extend to ensuring the risks at member schools are being assessed and addressed appropriately.

The risk climate can change rapidly. It is important emerging risks are carefully assessed and, where appropriate, are reflected in risk registers.

7. Risk Measurement (Assessing Likelihood and Impact) and Prioritisation

Once risks have been identified, it is important to measure them to give a standard for comparing the risks consistently. Measurement consists of assessment, evaluation and ranking. Having identified the risks that the school/Trust is facing, they are prioritised into a manageable order so that action can be focused on the significant risks.

The aim of assessment is to better understand each specific instance of risk and how it could affect business objectives. Each risk is assessed in terms of the **likelihood** (or probability) of its occurrence, and its **impact** (or severity) on the school/Trust, should it occur.

The impact of a risk and the likelihood of it occurring are scored as follows:

a. Likelihood

1. Remote
2. Unlikely
3. Possible (moderately likely)

4. Probable
5. Highly probable

b. Impact

1. Insignificant
2. Minor
3. Moderate
4. Major
5. Extreme/Catastrophic

The scores are multiplied for likelihood and impact and then ranked by numerical value.

Risk priority is interpreted as follows:

- Score of 15 or more: High priority risk (red)
- Score of 8-14: Priority risk (yellow)
- Score of 7 or less: Low priority risk (blue and green)

This can be represented as a risk matrix, or risk heat map:

Likelihood						
	5 - Highly Probable	5	10	15	20	25
	4 - Probable	4	8	12	16	20
	3 - Possible	3	6	9	12	15
	2 - Unlikely	2	4	6	8	10
	1 - Remote	1	2	3	4	5
		1 - Insignificant	2 - Minor	3 - Moderate	4 - Major	5 - Extreme
	Impact					

8. Risk Mitigation

Once risks have been identified, assessed and prioritised, the school/Trust will ensure that there are appropriate plans to address and manage them. These plans might include putting in place preventative controls, mitigation processes and contingency plans, if risks materialise.

The approach taken will depend substantially on the Trust's:

- **Risk appetite** – the amount of risk the Trust is willing to accept in the pursuit of its objectives; and
- **Risk capacity** – the resources (financial, human etc.) which the Trust is able to put in place in managing risk.

As an initial step, the school/Trust will assess the 'cost' of accepting the risk. This may be a financial cost or a lost opportunity. The school/Trust may decide that accepting a particular risk is appropriate and not take any further action.

If the school/Trust decides further action is needed, then there are five main options:

- **Treat the risk** – this involves controlling the risk with actions to minimise the likelihood of occurrence or impact.

- **Transfer all or part of the risk** – this may involve the use of insurance to mitigate risks or payment to third parties.

- **Terminate the risk** – this can be done by altering an inherently risky process to remove the risk.

- **Tolerate the risk** – this is where no action is taken.

- **Take advantage** – this recognises that the uncertainty attached to risk sometimes offers opportunities as well as threats.

Trustees will also consider that whilst a risk may be avoided by withdrawing from that area of activity, doing so may result in a missed opportunity.

A risk may be transferred wholly or in part to a third party, possibly through insurance or a partnership arrangement.

In the majority of cases, the next step will be to put in place systems to mitigate either the likelihood or the impact of the risk. These will include systems addressing the whole operation of the school/Trust, as well as the areas where risks have been identified. Any system of risk mitigation should provide as a minimum:

- Effective and efficient operation of the school/Trust.
- Effective internal controls.
- Compliance with law and legislation.

Mitigating action plans should be recorded against each risk that has been listed in the risk register with appropriate milestones. In order for an action plan to be successful the action plans should be:

- Specific
- Measurable
- Achievable
- Realistic
- Time constrained

They should also include sources of assurance over the controls in place to mitigate each risk identified.

Source of Assurance (see section 4) is defined as evidence that mitigating action/controls are in place and being regularly reviewed. As part of the monthly risk review the Assurance should be reviewed to ensure that the mitigating action/controls are appropriate and functioning. The residual risk should also be considered at each review if Assurances indicate that mitigating actions/controls are working better/worse than originally planned.

9. Gross and Net Risk

In completing the assessment of risk, recognition needs to be given to the impact of the mitigating actions taken to reduce the impact of the risk. Accordingly, risks will initially be recorded at their gross value which is the impact without mitigating actions. The same risks will then be recorded at their net value, allowing for the impact of the mitigating actions.

Both the gross risk and net risk scores are to be recorded on the risk register.

The movement in these risk scores between reporting periods are to be recorded to assess whether a risk is constant, decreasing or increasing over time.

10. Risk Monitoring

Monitoring should be ongoing and continuous as this supports the Trust's understanding of whether and how the risk profile is changing. The likelihood or impact of an identified risk can change for a number of reasons including:

- Nature of the risk has changed or is changing.
- Existing controls are inadequate or not functioning.
- New controls are introduced.

The risk register is central to risk monitoring. As risks are identified, they should be logged on the register and the associated control measures documented. A risk register is a live document.

11. Risk Reporting

Different levels within the Trust need different information from the risk management process. Information should be clear and support the Trust Board and FAR Committee to assess whether decisions are being made within their risk appetite, to review the adequacy and effectiveness of internal controls, to reprioritise resources and improve controls and to identify emerging risks.

Early warning indicators should be reported systematically and promptly to the appropriate level to allow action to be taken. The frequency of reporting should be related to how quickly a risk can materialise and its likely impact.

Trustees will form a view as to the acceptability of the residual risk that remains after risk management strategies have been implemented. In assessing additional action to be taken, the costs of management or control will generally be considered in the context of the potential impact or likely cost that the control seeks to prevent or mitigate. It is possible that the process may identify areas where the current or proposed control processes are disproportionately costly or onerous compared to the risk that they are there to manage. A balance will need to be struck between the cost of further action to manage the risk and the potential impact of the residual risk.

12. General

This policy is at the discretion of the Board of Trustees and can be varied at any time. In the event of any conflict with primary legislation or statutory regulations, the legal provisions will have precedence over this policy in all cases.