Bishop Chadwick Catholic Education Trust

Risk Management Policy

Document Management: Date Policy Approved: September 2021 Next Review Date: September 2024

Risk Management Policy

Purpose of this document

This Risk Management policy forms part of the internal control and governance arrangements of Bishop Chadwick Catholic Education Trust (the "Trust").

The policy explains the Trust's approach to risk management, documents the roles and responsibilities of the Trust Board and Accounting Officer. The document also outlines key aspects of the risk management process, and identifies the main reporting procedures.

In addition, it describes the process that will be used to evaluate the effectiveness of the Trust's internal control procedures.

Attitude to risk

In pursuing its objectives, as expressed in its Strategic Plan and elsewhere, the Trust will generally accept a level of risk proportionate to the expected benefits to be gained, and the scale or likelihood of damage.

The Trust has a low appetite for risk where there is a likelihood of significant and lasting reputational damage; significant and lasting damage to its provision of outstanding teaching and learning; significant financial loss or significant negative variations to financial plans; loss of life or harm to students, staff or visitors.

Approach to risk management

The Trust follows and adopts good practice in the identification, evaluation and control of risks to ensure that, as far as reasonably practicable, risks are avoided or reduced to an acceptable level. Although it is acknowledged that risks exist and can never be eliminated, it is important that the Trust Board, Local Governing Committee, Senior Management Team (meaning the Executive team and Academy Headteachers) and all employees are aware of risk associated with their area of work. The following key principles outline the Trust's approach to risk management:

- the Trust Board has responsibility for overseeing risk management within the Trust as a whole;
- Senior Management advise on and implement policies approved by the Trust Board and are responsible for encouraging good risk management practice within their areas of responsibility;
- key risks will be identified and monitored on a regular basis.

Risk identification

The process of risk identification will involve both Directors, the Executive Team (and wider Central Team) and Academy Headteachers and their respective Local Governing Committee.

Consideration will be given to the following factors:

- The vision, beliefs, values and strategic goals;
- The nature and scale of the Trust and constituent Academy's activities, both current and planned;
- External factors that may affect the Trust such as legislation and regulation;
- The Trust's reputation with its key stakeholders;
- The operating structure, e.g. functions and issues that the Trust may face, including those relating to academy conversion as part of the Diocesan Growth plan.

Role of the Board

The Trust Board, informed and advised by the Audit Committee, should:

- lead the assessment and management of risk and take a strategic view of risks in the organisation.
- ensure that there are clear accountabilities for managing risks and that officials are equipped with the relevant skills and guidance to perform their assigned roles effectively and efficiently.
- ensure that roles and responsibilities for risk management are clear to support effective governance and decision-making at each level with appropriate escalation, aggregation and delegation.
- determine and continuously assess the nature and extent of the principal risks that the organisation is willing to take to achieve its objectives - its "risk appetite" - and ensure that planning and decision-making appropriately reflect this assessment.
- agree the frequency and scope of its discussions on risk to review how management is responding to the principal risks and how this is integrated with other matters considered by the board, including business planning and performance management processes.
- specify the nature, source, format and frequency of the information that it requires.
- ensure that there are clear processes for bringing significant issues to its attention more rapidly when required, with agreed triggers for doing so.
- use horizon scanning to identify emerging sources of uncertainty, threats and trends.
- assure itself of the effectiveness of the organisation's risk management framework.

Role of the Accounting Officer

The Accounting Officer, supported by the Audit Committee, should:

- periodically assess whether the organisational values, leadership style, opportunities for debate and learning, and human resource policies support the desired risk culture, incentivise expected behaviours and sanction inappropriate behaviours.
- ensure that expected values and behaviours are communicated and embedded at all levels to support the appropriate risk culture.
- designate an individual to be responsible for leading the organisation's overall approach to risk management, who should be of sufficient seniority and should report to a level within the organisation that allows them to influence effective decision-making.
- establish the organisation's overall approach to risk management
- establish risk management activities that cover all types of risk and processes that are applied at different organisational levels.
- ensure the design and systematic implementation of policies, procedures and practices for risk identification, assessment, treatment, monitoring and reporting.
- consider the organisation's overall risk profile, including risk management within arm's length bodies and the extended enterprise.
- demonstrate leadership and articulate their continual commitment to and the value of risk management through developing and communicating a policy or statement to the organisation and other stakeholders, which should be periodically reviewed.
- ensure the allocation of appropriate resources for risk management, which can include, but is not limited to people, skills, experience and competence.
- monitor the quality of the information received and ensure that it is of a sufficient quality to allow effective decision-making.

- ensure that risk is considered as an integral part of appraising option choices, evaluating alternatives and making informed decisions.
- be provided with expert judgements through functions to advise on:
  - the feasibility and affordability of strategies and plans;
  - the evaluation and development of realistic programmes, projects and policy initiatives;
  - prioritisation of resources and the development of capabilities;
  - the design and operation of internal control in line with good practice and the nature and extent of the risks that the organisation is willing to take to achieve its objectives; and
  - driving innovation and incremental improvements.
- clearly communicate their expectation that risk management activities are coordinated and that information is shared among across the 'lines of defence' where this supports the overall effectiveness of the effort and does not diminish any of the 'lines' key functions.

Risk management and the systems of internal control

The Trust's risk management policy includes systems of internal controls. These controls encompass a number of elements that together facilitate an effective and efficient operation, enabling the Trust to respond to a variety of operational, financial, and commercial risks. These elements include:

Policies and procedures

Attached to significant risks are a series of policies that underpin the internal control process. The policies are approved by the Trust Board and implemented and communicated by the Executive Team to all staff via Academy Headteachers. Written procedures support the policies where appropriate.

Regular reporting

Regular reporting is designed to monitor key risks and their controls. Decisions to rectify problems identified are made at regular meetings of the Local Governing Committee or Trust Board as appropriate.

Risk Register

The Audit Committee is responsible for overseeing the compilation and termly review of an overall Risk Register to facilitate the identification, assessment and ongoing monitoring of major risks to which the Trust is exposed. Emerging risks are added as required, and improvement actions and risk indicators are monitored regularly. The Trust Risk Register includes risks pervasive to the Trust and specific risks relating to individual academies where assessed as high risk.

The Risk Register is maintained/reviewed in accordance with the Academy Trust Handbook which states:

- Overall responsibility for risk management, including ultimate oversight of the risk register, must be retained by the board of trustees, drawing on advice provided to it by the Audit Committee.
- Other committees may also input into the management of risk at the discretion of the board.
- Aside from any review by individual committees, the board itself must review the risk register at least annually.
- Risks management covers the full operations and activities of the trust, not only financial risks.

Internal scrutiny programme

The Academy Trust Handbook states that all Academy trusts must have a programme of internal scrutiny to provide independent assurance to the board that its financial and non-financial controls and risk management procedures are operating effectively.

The Academy Trust Handbook allows a number of options re the delivery of internal scrutiny:

- employing an in-house internal auditor;
- a bought-in internal audit service from a firm, other organisation or individual;
- with professional indemnity insurance;
- the appointment of a non-employed trustee;
- a peer review by the chief financial officer from another academy trust.

The Trust has assessed that, recognising the size and complexity of the organisation, the most appropriate option is provision of internal audit services by an member of a relevant professional body.

External audit

External audit of the financial statements provides feedback to the Trust Board on the operation of the internal financial controls reviewed as part of the annual audit. Other external audits (e.g. health and safety, may also be the subject of periodic reports to the Trust Board.

Annual review of effectiveness

The Trust Board is responsible for reviewing the effectiveness of internal control of the Trust. The Audit Committee reviews the Risk Register each term and considers the internal and external risk profile of the coming year and consider if current internal control arrangements are likely to be effective.

References

- The Academy Trust Handbook
- Charity Commission guidance on Charities and Risk Management
- HM Government's Orange Book (Management of Risk- Principles and Concepts)

Linked policies

- Finance Policy
- Business Continuity Policy
- Budget Forecasting and Monitoring of Reserves Policy
- Estates Management Plan
- Data Protection Policy
- Information & Cyber Security Policy
- Safeguarding & Child Protection Policy
- Attendance Policy
- Health & Safety Policy
- Business Continuity Plan

Appendix 1 – Example Risk Categories

The following list, which is not exhaustive, is as per Annex 4 of HM Government's Orange Book (Management of Risk- Principles and Concepts).

Strategy 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).

Property risks - Risks arising from property deficiencies or poorly designed or ineffective/inefficient safety management resulting in non-compliance and/or harm and suffering to employees, 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. Failure to manage risks in any of these categories may lead to financial, reputational, legal, regulatory, safety, security, environmental, employee, customer and operational consequences.