UNIVERSITY OF OXFORD

RISK MANAGEMENT POLICY

INTRODUCTION

There is a degree of risk involved in all our activities. Understanding the risks we face and managing them appropriately is critical to fulfilling our mission of "the advancement of learning by teaching and research and its dissemination by every means". Effective identification and management of risk protects our teaching and research, our people (staff, students and visitors), our resources and our reputation. Understanding and mitigating our risk also enhances the University's ability to make better decisions, respond quickly and effectively and exploit opportunities.

PURPOSE

This Policy sets out the University's objectives and strategy for risk management, and the arrangements it has adopted to enable it to manage its risks. The aim of the policy is not to eliminate risk from the University's activities, but rather to ensure that every effort is made to manage risk appropriately and in line with the University's risk appetite. The policy also defines roles and responsibilities in relation to risk management and the processes for reporting risk within the University.

OBJECTIVES

The University's objectives for risk management are:

a) to align risk management with the University's objectives (as set out in the Strategic Plan and elsewhere);

b) to appraise and manage risks and opportunities in a systematic, structured, timely manner and in accordance with the University's Risk Appetite Statement; to ensure that there is clear accountability and responsibility for risk within the University and that risks are managed at the most appropriate level.

SCOPE

This Policy has been adopted by Council and applies throughout the University apart from Oxford University Press, which has its own policy and procedures for risk management. This policy also applies in full to wholly-owned and majority owned subsidiary companies and joint ventures unless separate policies have been formally approved and adopted by the Boards of those companies and endorsed by the Council's General Purposes Committee.

DEFINITIONS

- ***Risk*** is anything that can endanger the achievement of our mission or potentially damage our reputation. Risks can be either threats or opportunities missed.
- ***Risk Appetite*** is the high-level view of the total level of risk the University is willing to take to achieve its objectives.
- ***Risk Management*** is the systematic process of identifying, evaluating, managing and monitoring risks and developing mitigating actions so that our mission can be achieved.

RISK APPETITE

The University's statement of risk appetite guides the University's approach to the acceptance of risk. The University's current Risk Appetite Statement is included at Appendix 1.

RISK MANAGEMENT PRINCIPLES

Risk management at the University operates according to the following principles:

- Risk management is a continuous process and embedded in day-to-day operations. All staff actively engage in risk management in their areas of responsibility as and when required. Risk is managed both informally through good day-to-day operational management and decision making and also formally through a structured assessment process.
- The escalation of risk information is timely, accurate and insightful. Risks are assessed collectively and collaboratively and the information is used to support planning and decision making at all levels and to inform stakeholders.
- 'Top-down' and 'bottom-up' risk assessments are integrated to produce a comprehensive picture of risk across all University activities.
- The University captures, considers and treats risk in an effective and efficient manner with proportionate processes and procedures. Significant risks across the University are assessed and documented by the Divisions and Main Committees according to standard processes and consistent impact and likelihood scoring. This is necessary for the information to be aggregated and reviewed. Minor/ localised risks are documented and managed by the relevant Department/ Faculty/ other academic or service unit with more flexibility for local determination of the appropriate tools and processes.

RISK REGISTERS

A 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. Risk registers are held by each of the Divisions and Main Committees of the University and are regularly updated and reviewed by the relevant Committee/Divisional Board.

When updating and reviewing risk registers Committees and Divisional Boards are mindful of the current Risk Appetite Statement (Appendix 1), ensuring for example that controls and mitigations are robust for risks where the university has an averse or cautious approach.

Faculties, departments, and other academic and service units of the University are also encouraged to hold their own risk registers but this is not mandatory. Divisions and Main Committees ensure that they have appropriate mechanisms in place to collect information on risk identification and management from relevant faculties, departments and other academic and service units.

Further guidance on the production and maintenance of risk registers is available from the Risk Management section of the University website: https://compliance.admin.ox.ac.uk/risk-management.

UNIVERSITY RISK REGISTER (URR)

The University Risk Register is a summary of the key risks facing the University as a whole, and is the document used by Council, General Purposes Committee and Audit and Scrutiny Committee to monitor and manage risk.

The URR is updated twice annually by the review and aggregation of risk registers submitted by the Divisions and Main Committees of the University to the Assurance Directorate. The URR also informs the Risk Management Statement in the University's Financial Statements.

ROLES AND RESPONSIBILITIES

All staff have a 'front line' responsibility for identifying, evaluating and managing risk within their area of responsibility. They should assist with the implementation of risk mitigation strategies relevant to their role. All staff should escalate upwards any concerns regarding new or existing risks within their department/ division/ faculty or service.

Risk owners are responsible for ensuring specific risks are appropriately identified, assessed and mitigated. They input into the risk register and liaise with owners of specific controls and actions to ensure they are implemented. The appointed risk owner will be a senior member of staff within the appropriate unit of the University e.g. a Pro-Vice-Chancellor, Registrar or a Director.

Divisional Boards and Main Committees are responsible for the identification, evaluation, management and reporting of risk within their area of responsibility (including any risks shared with third parties such as the Colleges, Private Permanent Halls and NHS). They update and review their Divisional/ Committee risk registers, ensuring risk is managed in line with the University's risk appetite. They obtain input as needed to their risk register from individual risk owners, departments, faculties and other academic and service units of the University.

Heads of Department, Faculty Board Chairs and Heads of University Services are responsible for implementing this policy within their area of responsibility. They should ensure that processes are in place for the identification, evaluation, management and reporting of risk (including any risks shared with third parties such as the Colleges, Private Permanent Halls and NHS). They ensure risk is managed in line with the University's risk appetite. They share risk identification and management information with their Division/ relevant Main Committee.

The **Boards of Directors of wholly-owned and majority owned subsidiary companies and joint ventures** of the University are deemed to have responsibilities equivalent to Heads of Department as set out above unless alternate arrangements have been agreed and approved by GPC.

The Boards of Directors of equal and minority joint ventures are expected to act in accordance with this or equivalent policies.

Council is ultimately accountable for risk management and determines the nature and extent of the significant risks it is willing for the University to take in achieving its objectives as well as ensuring sound risk management and internal control systems exist. It sets the risk management direction and risk appetite, challenges the risk management process and key risks reported to it, gathers assurance on the process and ensures appropriate communication on risk is made to stakeholders. However, it delegates responsibility for the implementation of risk management to the General Purposes Committee and monitoring to the Audit & Scrutiny Committee.

General Purposes Committee (GPC) is responsible for applying the risk management process across the University on behalf of Council. It ensures that processes and responsibilities have been clearly established and recommends changes to risk management policy to Council. It assesses and manages

the University's most significant risks (including identification of new risks and review of cross-cutting issues), directs management's risk management activities and reports risk information to Council.

The **Audit and Scrutiny Committee** (ASC) provides independent assurance to assist Council in fulfilling its responsibilities for ensuring ~~on~~ the adequacy and effectiveness of the University's arrangements for risk management. It receives internal audit reports and the URR and reports its assessment to Council. It reviews the University's Financial Statements to ensure accurate public-facing description of risks.

The **Assurance Directorate** facilitates the formal risk management process throughout the organisation and enables the reporting of risk information to GPC, ASC and Council. This includes updating the risk management process and tools, and providing training to support this policy. The Assurance Directorate consolidates Divisional and Main Committee risk registers to produce the University Risk Register and drafts the Risk Management Statement for the University Financial Statements. It also obtains input on risk from other key stakeholders e.g. legal and insurance contacts.

The **Assurance Management Group** (AMG) reports to Audit and Scrutiny Committee and assists it in fulfilling its responsibilities, including as regards risk management. The AMG reviews and endorses the draft Risk Management Statement for the University Financial Statements.

The **internal auditors** undertake audit work sufficient to allow them to provide an annual opinion to ASC on the adequacy and effectiveness of the University's arrangements for risk management. They also audit specific areas of risk as directed by the internal audit plan and report on the adequacy of controls and areas for improvement to ASC.

INTERACTION WITH OTHER POLICIES, PROCEDURES AND REGULATION

This Policy takes account of the University's wider legislative obligations as they relate to risk management, including the Conditions of Registration with the Office for Students (OfS) and the OfS's Accounts Direction.

The University is also mindful that this Policy interacts and overlaps with a number of other University policies and procedures, including but not limited to:

- Financial Regulations and supporting Financial Processes including, in particular; insurance;
- Health and Safety Policy and associated Regulations and Codes;
- Research Integrity and Ethics;
- Bribery and Fraud Policy;
- Information Security Policy and associated controls relating to IT risk.
- Business Continuity Policy

INTERACTION WITH THIRD PARTIES

In order to achieve its objectives, the University works closely with a number of third parties, including the colleges, the Permanent Private Halls and the NHS. Some risks are therefore shared with these third parties.

Whilst GPC retains an overview of the University's strategic relationships, where divisions and departments have significant interaction with third parties, it is the responsibility of the Head of Division

or Head of Department (as appropriate) to ensure that adequate steps are taken to manage shared risks effectively.

FURTHER GUIDANCE

Further guidance and templates to implement this policy are provided on the Risk Management section of the University website: https://compliance.admin.ox.ac.uk/risk-management

Policy approved by General Purposes Committee of Council on: 26 June 2023

Policy due for review: TT2026

APPENDIX 1: Risk Appetite Statement

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

Risk appetite is the level of risk exposure that the University is prepared to accept or willing to take in pursuit of its strategic objectives.

University statement of risk appetite

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

The University has a high appetite for risk in the context of encouraging and promoting critical enquiry, academic freedom, freedom of expression, and open debate.

The University has a very low appetite for risk where there is a likelihood of significant and lasting reputational damage; significant and lasting damage to its provision of world-class research or teaching; significant financial loss or significant negative variations to financial plans; loss of life or harm to students, staff, collaborators, partners or visitors; or illegal or unethical activity.