Risk Management Policy

1. Purpose and definitions

1.1 The purpose of the risk management policy is to explain the University's underlying approach to risk management and to document the roles and responsibilities of the Board and its sub-committees, the University's senior leadership and other staff with executive responsibilities. It also outlines key aspects of the risk management process and identifies the main reporting procedures.

1.2 Corporate risks are recorded in the University Strategic Risk Register. This records opportunities or threats that may affect the University's future success and ability to deliver its strategic plan. The Register is a dynamic and 'living document' that is populated and updated through the University's regular risk assessment and management work. It provides an assessment of the potential magnitude or scale and likelihood of a given risk and details of how individual risks will be treated, the controls in place to mitigate the risk and plans to strengthen the controls.

2. Scope and approach to risk management

2.1 This risk management policy forms part of the University's governance and internal control arrangements.

2.2 The University has a responsible approach to risk management, seeking to recognise and manage appropriately its exposure to risks. In pursuit of achieving its strategic aims and academic mission the University will, therefore, accept a degree of risk, commensurate with the potential reward.

2.3 Risk management is embedded into the management practice of the University's senior leadership. This approach is championed by the Vice Chancellor and is reflected in the Vice Chancellor's reports, presented at each meeting of key University committees and meetings, namely: The Board, the University Executive Board, the University Leadership Group and briefing meetings for all staff.

3. Risk Appetite

3.1 The risk appetite framework, describes the level of risk that the University is willing to accept in the pursuit of its strategic aims and long term objectives, and will inform formal strategic decision-making by the Board. Therefore, risk appetite seeks to articulate and prioritise institutional effort and balance the institutional risk profile in key strategic areas, to ensure that the University's resources and creativity are focused on key areas (known as 'Key Risk Areas'). In order to facilitate innovation, to enable the University to be sector-leading, to develop new models of working and/or to embrace new opportunities in areas central to its mission and strategy, the University is willing to tolerate more risk-taking, with appropriate mitigating action. In other areas of activity, the University will be more cautious and less willing to take risks.

3.2 The University's Key Risk Areas in the risk appetite framework are:

- Regulatory and Compliance
- Financial
- Sustainability
- Reputation
- People and Culture
- Information (including Cyber Security)
- Learning, Teaching and Student Experience

- Research and Knowledge Exchange
- Government Policy/External Environment

These will be reviewed regularly to ensure they remain aligned with the University's strategic plan.

3.3 The risk appetite thresholds are of relative rather than absolute measures. The thresholds are as follows:

Classification	**Description**
Adverse	Avoidance of risk
Cautious	Preference for very safe options. Very low degree of inherent risk. Potential rewards therefore likely to be low
Moderate	Preference for safe options. Low degree of inherent risk. Potential rewards therefore likely to be limited
Open	Preference for options which offer greater potential reward. Willing to accept greater inherent risks
Hungry	Preference for innovative options. Highest possible rewards and inherent risks

3.4 The Key Risk Areas and Risk Appetite Thresholds are reviewed and approved on at least an annual basis at times, when the Board is reviewing the delivery of the Strategic Plan and setting priorities for the academic year (Appendix 1)

4. Responsibilities

4.1. The **Board** is responsible for:

- Approving the Risk Management Policy
- Reviewing annually the University's approach to risk management and risk appetite
- Approving changes or enhancements to key element of its processes or reporting, except those decisions for which the Audit Committee has delegated powers (see 3.2 below).
- Seeking assurance (via Audit Committee) of the successful implementation of the Risk Management policy and related processes
- Reviewing the University Risk Register at least twice times per annum and approving as appropriate changes proposed to the Register
- Monitoring the management of all corporate risks by the University's senior leadership
- Approval of major decisions affecting the University's risk profile or exposure.

4.2 In accordance with sector-wide requirements, the **Audit Committee** is responsible for:

- Reviewing the effectiveness of the risk management, control and governance arrangements on behalf of the Board.
- Reporting to the Board on internal controls and alerting members to any emerging issues.
- Monitoring, on behalf of the Board, the management of corporate and department-level risks, by receiving and reviewing risk management reports (including the University Strategic Risk Register) at least two times per annum. The Reports shall summarise the review process and any key themes that have been identified.
- Authorising remedial action where necessary to enhance the University's risk management arrangements.
- Providing comment on new risks.

4.3 Led by the Vice-Chancellor and Chief Executive, **University's Senior Leadership** team (known as the University Executive Board (UEB) is responsible for:

- Identifying, evaluating and reporting the significant corporate risks faced by the University, and ensuring that appropriate mitigating action is taken. The team is responsible for monitoring and reporting changes in the status of corporate risks, in risk management reports and the University Risk Register for consideration by the Board and the Audit Committee.

- Providing adequate information in a timely manner on the status of risks, controls and planned action.
- Undertaking training and development activities associated with risk management, as appropriate.

4.4 Individual **members of the University's Leadership team** are responsible for:

- Effective risk management in their areas of responsibility, in accordance with the University's Risk Management Policy and procedures.
- Undertaking regular reviews and assessment of key risks within their areas of operation as part of routine management arrangements. Overseeing the implementation of risk management controls and planned development work in their area of responsibility.
- Escalating any significant changes in terms of existing or new risks to the University's Risk Manager through regular updates to Departmental Risk Registers

4.5 The **University's Risk Manager** is responsible for ensuring that the University operates effective procedures relating to risk management and for undertaking formal reviews on behalf of the Board of the risk management policy. The Risk Manager will maintain the University Strategic Risk Register and will be responsible for its update prior to the review by UEB. The Risk Manager will provide on-going training to risk owners in order to facilitate the effective operation of risk management and prepare risk management reports on behalf of the University's senior leadership for consideration by both the Board and the Audit Committee. This responsibility currently resides with the Head of Governance and Regulatory Affairs.

4.6 **Responsibility for identifying risks** to be added to the University Strategic Risk Register rests primarily with the University Risk Manager. They are responsible for identifying any matters shown on local risk registers (department, project and IT/Cyber Security) which could impact on strategic risks in terms of their ratings and to reflect these in the Strategic Risk Register accordingly. The overall process for updating risk register with indicative timelines is set out at Appendix 2. In addition, as part of the half yearly review UEB will consider the wider national, and international, context that the University is operating in and whether any changes need to be made to the Strategic Risk Register to reflect this.

5. Risk Identification and Assessment

5.1 The methodology used to assess Corporate Risks in the University Risk Register is based on the use of a nine-point scale risk rating mechanism to assess the impact and likelihood of risk, based on the following definitions:

	Impact		
Likelihood	**MINOR**	**MODERATE**	**MAJOR**
UNLIKELY	LOW Accept the risk Routine Management	LOW Accept the risk Routine Management	MEDIUM Specific responsibility & treatment
POSSIBLE	LOW Accept the risk Routine Management	MEDIUM Specific responsibility & treatment	HIGH VCEB Review, at least quarterly
LIKELY	MEDIUM Specific responsibility & treatment	HIGH VCEB Review, at least quarterly	EXTREME VCEB scrutiny at 90%+ of meetings

5.2 Classifications of extreme. high, medium and low impact and likelihood are provided below:

	EXTREME	HIGH	MEDIUM	LOW
IMPACT	• Critical impact on the University with strong risk of organisation failure	• Result in significant impact on the University's financial sustainability and/or • Inability to achieve one or more strategic aims or objectives, and/or • Significant reputational damage	• Restrict ability to achieve one or more strategic aims or objectives	• Impact on some aspects of one or more strategic aims or objectives
LIKELIHOOD	Greater than 90% chance of the risk materialising in the next 2 years Or risks which are out of the University's control	Between 70% to 90% chance of the risk materialising in the next 2 years	Between 30% to 70% chance of the risk materialising in the next 2 years	Less than 30% chance of the risk materialising in the next 2 years

6. Risk Reporting

6.1 The University has four types of risk register:

- **University Strategic Risk Register**: this Register is intrinsically linked to the University Strategic Plan. It identifies risks that have a fundamental impact on the University's ability to operate as a business and/or deliver its Strategic Plan. Risk management is incorporated into the strategic planning process to ensure that the University is able to monitor risks to achieving the University's objectives and determine which risks have the most significant impact.

- **Departmental Risk Registers**: these Registers are owned by Heads of Department, and their SMTs, and documents the risks and risk management activity associated with the operation of the department. These are reviewed twice a year by Heads and submitted to the University Risk Managers as part of the six month review of the University Strategic Risk Register.

- **Local Risk Registers***:* The high-level strategic risks identified in the University Risk Register, are underpinned and informed by specific risk registers managed at the local operational level. There are currently registers for major University projects including refurbishment and construction of buildings and the Medical School project, as well as a Covid 19 Risk Register.

- **IT/Cyber Security Risk Register**: owned by IT, this documents risks and risk management activity associated with the University's IT infrastructure and information security. This is reviewed twice a

year by the Information Governance Group and VCEB and presented to Audit Committee at least once a year for review.

6.2 Format of Risk Registers

6.2.1 The University Risk Register and Local Risk Registers share common features to ensure a consistent approach to risk identification and risk management across all areas. Each register incorporates the following criteria:

CRITERIA	DETAIL
Risk ID	Provides the risk with a unique identifier
Risk Event	A short description of something that might happen that would indicate a failure to achieve, or an impediment to achieving a strategic objective or goal
Cause	There are often multiple causes for a given risk event
Impact	The possible impact on the University should the risk event occur
Gross risk rating	The gross risk rating is a combination of the likelihood of the risk happening and the impact should not mitigating actions be taken. These are graded Extreme to Low as set out in the Risk Matrix at para 5
Risk Owner	A member of VCEB whose area the risk falls into either directly or through line reports. It is the responsibility of the risk owner to ensure that actions are being implemented and appropriate reports made to VCEB.
Mitigating Actions	Broad actions which will be undertaken to mitigate the risk. These will often be expanded in the Operational Plan or area specific Risk Registers and Action Plans.
Net Risk Rating	The net risk rating is a combination of the likelihood of the risk happening and the impact once the mitigating actions have been taken. These are graded Extreme to Low as set out in the Risk Matrix at para 5 and the reporting requirements identified in the Risk Matrix related to the Net Risk Rating

7. Risk Assurance Map

7.1 The Risk Assurance Map identifies how the risk management controls are being monitored in terms of their successful operation and effectiveness. For each risk three lines of assurance are mapped:

- First line: ongoing management responsibilities, relevant policies, procedures, and processes and/or management information reports
- Second line: internal structures and post-holders without direct management responsibilities in the specific business area that have a review/monitoring role, such as governance committees and senior manager with oversight responsibilities and success measures (where possible benchmarked with other Universities), associated with specific aims and objectives in the Strategic Plan 2019, which will be monitored by the Board
- Third line: independent reviews within the past three years by internal or external auditors (denoted by IA and EA respectively in table below) and external reviewer by designated sector bodies, regulators and professional accreditation bodies.
-

7.2 The Risk Assurance Map will be updated alongside the Risk Register in line with the Responsibilities set out at Para 4.

8. Internal and External Audit Procedures (as they relate to risk)

8.1 ***Internal Audit:*** Internal audit is an important part of the internal control process for risk. The University's internal auditors use a risk-based methodology, which is informed by the risks included in the risk register and a review of the Risk Assurance Map. Reviews of the University's approach to risk management (including the benefits that are derived) are undertaken on an annual basis and informed by a dedicated review of risk management every three years.

8.2 ***External Audit:*** External audit provides feedback to the Audit Committee on the operation of the risk management process on an ad hoc basis.

Owner	Head of Governance and Regulatory Affairs
Approved by	Board of Governors
Issue Date	July 2019, revised Oct 2020
Review Date	Jul 2021
Version	2.2
Accessibility checked	October 2020

Appendix 1

Risk Appetite Framework

	Adverse	Cautious	Moderate	Open	Hungry
Regulatory & Compliance					
Financial					
Sustainability					
Reputation					
People & Culture					
Information (incl Cyber Security)					
Learning, Teaching and Student Experience					
Research & Knowledge Exchange					
Government Policy/External Environment					

Process for updating risk registers (with indicative timings)