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 University's Risk Appetite is set out in the University's Risk Appetite Statement (Appendix 2)

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 elements of its processes or reporting, except those decisions for which the Audit Committee has delegated powers (see 4.2 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:

- Considering the wider national, and international, context, that the University is operating in and to identify, evaluate and report the significant corporate risks faced by the University; ensuring that appropriate mitigating actions are taken.
- Providing adequate information in a timely manner on the status of risks, controls and planned action.
- Ensuring that planned actions for the strategic risks assigned to them are being implemented
- Undertaking training and development activities associated with risk management, as appropriate.

4.4 The **University Secretary** is responsible for ensuring that the University operates effective procedures relating to risk management including:

- Ensuring that the Risk Management Policy is implemented and maintained;
- Ensuring that the Strategic Risk Register is maintained and updated on a regular basis (see Appendix 1), not less than twice a year taking into account updates from Operational Risk Registers and updates from members of the UEB;
- Ensuring that changes to the Strategic Risk Register, and areas of concern arising out of the half yearly review of Operational Risk Registers, is escalated and reported to the UEB, Audit Committee and the Board of Governors as appropriate;
- Providing appropriate levels of explanatory guidance and training to support the implantation of this Policy;
- Defining and implementing procedures for reporting and escalation of risk to the UEB, Audit Board and Board of Governors as required;
- Raising awareness of this Policy and its requirements amongst staff and all others to whom it is relevant

The University Secretary is supported in this work by the Risk Management and Business Continuity Officer.

4.5 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 Secretary through regular updates to Operational Risk Registers. The timeline for providing regular updates is set out at Appendix 1.

4.6 The **Boards of Directors of wholly owned subsidiary companies** of the University are deemed to have responsibility for:

- Ensuring that this Policy is implemented by the subsidiary company
- Ensuring that appropriate Operational Risk Registers are maintained in their respective areas and new, emerging and increasing risks are communicated to the University Secretary
- Ensuring that all those involved in the running of the subsidiary company are made aware of this Policy, and any requirements of that the Policy places upon them or their activities.

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 UEB Review, at least quarterly
LIKELY	MEDIUM Specific responsibility & treatment	HIGH UEB Review, at least quarterly	EXTREME UEB scrutiny at 90%+ of meetings

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.

- **Operational Risk Registers**: these Registers are owned by Heads of Academic Schools and Professional Department, and their SMTs, as well and the Board of the University's wholly owned subsidiary companies. They document 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 Prevent Duty 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 UEB and presented to Audit Committee at least once a year for review.

6.2 Format of Risk Registers

6.2.1 The University Strategic Risk Register and Operational Risk Registers share common features to ensure a consistent approach to risk identification and risk management across all areas.

6.2.2 The Risk Register Template uses Excel and provides for three worksheets:

- High Residual Rated Risks
- Medium Residual Rated Risks
- Low Residual Rated Risks

Each register incorporates the following criteria:

CRITERIA	DETAIL
Risk ID	Provides the risk with a unique identifier
Risk Description and Owner	A short description of the potential risk along with the Owner(s) of the risk. Owners should be the senior colleague(s) who is responsible for this risk within UEB or a School/Department SMT. If addressing the risk is dependent upon a different department taking an action then the Risk Owner is responsible for liaising with that department and raising their concern. The other department should not be identified as the Risk Owner
Initial risk rating	The initial risk rating is a combination of the likelihood of the risk happening and the impact should no mitigating actions be taken. These are graded Extreme to Low as set out in the Risk Matrix at para 5, these can be chosen from the drop-down lists and the overall risk rating will automatically be calculated and filled in.
Key Existing Controls	These are the key existing controls already in place to manage the risk
Residual Risk Rating	The residual risk rating is a combination of the likelihood of the risk happening and the impact once the key existing controls have been taken. These are graded Extreme to Low as set out in the Risk Matrix at para 5 - these can be chosen from the drop-down lists and the overall risk rating will automatically be calculated and filled in.
Risk Status since last review	This allows the risk owner to indicate whether the risk has increased, decreased, is unchanged or is tolerated. If a risk is new or is to be deleted than this can also be selected using the drop-down list. Note: if the risk rating has increased or decreased then the risk needs to be moved to the appropriate worksheet manually

Key Risk Theme and Risk Appetite Range	Each risk should be categorised against one or two of the Key Risk Themes identified in the Risk Appetite Statement and Matrix using the drop-down list.
Current and Planned Actions (not required for Low Residual Risks)	These are further planned controls which have either been identified or are in the process of being implemented to provide additional control to mitigate risks. Indicative timescales should be included where known. There will be risks which are outside of the University's or departments' control either completely or partially e.g. unknown government policy. In these cases the University or department will need to tolerate the risk but put in place, where possible, controls to mitigate the impact should the risk occur.
Action Due Date (Not Required for Low Residual Risks)	The date when it is anticipated the Action will be completed
Update on actions/mitigations (Not Required for Low Residual Risks)	This is so an update on progress can be provided on a regular basis when the management team is considering the risk and how it is being managed.

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

7.1 ***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 Strategic Risk Register. 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.

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

Owner	University Secretary
Approved by	Board of Governors
Issue Date	July 2019, revised Oct 2020, revised Oct 2021, revised Nov 2022 & Nov 2023 Revised January 2025 to reflect new format of Risk Register
Review Date	January 2028
Version	2. 5
Accessibility checked	November 2022

Appendix 1

Process for updating risk registers (with indicative timings)