Title	Risk Management Policy
Category	Corporate
Reference	Corp-RMP
Author(s)	Tony Saunders, Director of Finance and Chief Operating Officer Louise Bearder, Head of Clinical Governance
Responsible Director	Tony Saunders
Approved by	Audit and Risk Committee
Date issued	October 2025
Version	3.0
Next review due	October 2028

Version control

Version	Date issued	Brief summary of changes
1.0	July 2021	
2.0	July 2024	Review – no major changes
3.0	October 2025	New risk process, strategic risks and Vantage

1. About this policy

1.1 Risk is the uncertainty surrounding events and their outcomes in any area of St Luke's operations that may have a significant impact, both positive and negative, on the charity. The risk management arrangements form part of the wider system of internal control and should be understood in that context.

1.2 The objective of this policy is to provide a framework for managing risk to support the achievement of St Luke's strategic objectives, protect all the people who work for, volunteer for, use the services of and come into contact with St Luke's, and to safeguard our charity assets and good name to ensure the ongoing operation of St Luke's and long-term financial sustainability. More specifically the aim is to:

- Enable the early mitigation of threats and/or maximisation of opportunities in order to support the achievement of strategic objectives;
- Identify the major risks that apply to St Luke's and how to respond;
- Embed a consistent approach to risk management which is a key part of day-to-day operations; and
- Ensure that St Luke's meets its statutory and regulatory responsibilities relating to risk management and adheres to industry good practice.

Through having a comprehensive, consistent and clear approach to risk management, this will help create a culture of better decision-making and one in which innovation is encouraged by being risk-aware rather than risk-averse.

1.3 This policy has been developed in line with Charity Commission guidance (CC26) and other key regulatory bodies and provides a framework to:

- Define risk governance (Section 2)
- Identify, assess and mitigate principal risks (Section 3)
- Monitor, review and communicate risk activities (Section 4).

2. Risk Governance

The following table provides an overview of the responsibilities held at St Luke's for ensuring that this policy, and by extension our risk management environment, is both appropriate to the nature and scale of the charity and is effectively managed.

Group	Responsibilities
Board of Trustees	The Board is required to identify and review the reputational, regulatory, financial, innovation and quality, people and governance risks to which St Luke's is exposed and to assess the likelihood of such risks and the possible level of impact they would have. The Board must be satisfied that risk management is embedded in the organisation and adequate systems are in place to monitor, manage and, where appropriate, mitigate St Luke's exposure to the major risks. In discharging these duties, the Board delegates the detailed scrutiny of the risk environment and controls to the Audit and Risk Committee. However, the Board as a whole remains responsible overall for risk management and Trustees must ensure that they are satisfied that their duty is being fulfilled. The Board is responsible for setting the overall risk appetite of the organisation and the level of risk appetite associated with the principal areas of risk.
Audit and Risk Committee (ARC)	The ARC can make decisions as a collective group of trustees, executive and senior managers of St Luke's, within the delegated powers ascribed to it by the Board. The Executive leads, with the support of external, independent audit expertise as required and internal expert advice provide assurance to the ARC on overall risk management arrangements. The ARC receives, considers and advises on any risk management issues referred to the Committee by the Executive, Senior Managers and independent advisers.

	The ARC Receives reports on the effectiveness of risk management, reviews the overall risk framework and makes recommendations on any amendments, and regularly reviews and interrogates the Corporate Risk Register via the Board Assurance Framework. The ARC escalates risk matters for discussion by the Board as appropriate and advises the Board as to the effectiveness of the risk framework.
Healthcare Governance Committee (HGC), Resource and Finance Committee (R&F), Nominations and Renumerations Committee (NRC) and Research Committee	The HGC considers the clinical risks, recommends and reviews detailed reports on selected clinical risks, and escalates clinical risk matters for discussion at ARC and the Board as appropriate. The R&F Committee considers financial, estates related, HR, legal, income generation and other resourcing risks and escalates corporate risk matters for discussion at ARC and the Board as appropriate. The Research Committee considers research and education related risks and escalates risk matters identified in these areas for discussion at ARC and the Board as appropriate. NRC would escalate specific risk issues related to the committee's activities.
Executive team	The Chief Executive Officer is responsible for overall organisational risk management and so must gain assurance that risks are being appropriately and effectively managed. The Chief Executive Officer delegates the day to day management of the corporate risk register and associated processes to the Director of Finance and Chief Operating Officer. The Director of Finance and Chief Operating Officer is responsible for planning, overseeing, developing and reporting on the corporate risk register and is responsible for ensuring risk management issues are discussed regularly by the Executive Team and are escalated to the Chief Executive Officer, the Audit and Risk Committee, and the Board of Trustees as appropriate. The Executive team promotes risk management processes throughout the organisation and encourages transparency in reporting and speedy issue and risk escalation. Each Director is responsible for regularly reviewing and considering all areas of risk within their directorate and for escalating new or increased risk factors to the Director of Finance and Chief Operating Officer as and when they are identified.

Head of Clinical Governance & Head of Operations	Oversee the Clinical and Non-Clinical operational risk registers respectively and produce relevant reports to ARC and other committees as required. Work with the Director of Finance and Chief Operating Officer to manage and populate the BAF.
OLT	Each OLT member is responsible for the operational risk register within their area and working with the Executive Lead to identify and manage operational risk.
Managers and staff	All employees must comply with risk management policy and processes and foster an environment where risks can be identified and escalated.

3. Identifying, assessing and mitigating principal risks

3.1 Whilst acknowledging that it is impossible to eliminate risk and uncertainty, or to have systems and controls that provide 100% protection, St Luke's ambition is to have a proportionate response that would be objectively viewed as 'good'.

3.2 Risk is embedded within the organisation and risk management is factored into business planning, performance management, audit and assurance, business continuity management and project management.

3.3 There are a myriad of risks to which St Luke's is exposed. In order to aid risk management, the risks facing St Luke's are split between seven main categories:

- Reputation
- Regulation
- Finance
- Innovation and quality
- People
- Governance
- Projects.

3.4 The purpose of introducing categories is to stimulate thinking and ensure that a comprehensive list of potential risks is developed.

3.5 There will be 3 overall tiers of risk management;

    i.   **Strategic Risks** – These are the key themes that could prevent St Luke's from achieving its Strategic objectives. Each Corporate and Operational Risk will link to at least one Strategic Risk.

ii.   **Corporate Risk Register** – These are organisation wide, high-level risks held primarily by the Executive Team.

iii.   **Operational Risk Registers** – These are department/area specific risks that are primarily managed by the OLT. These may be escalated on to the Corporate register if necessary.
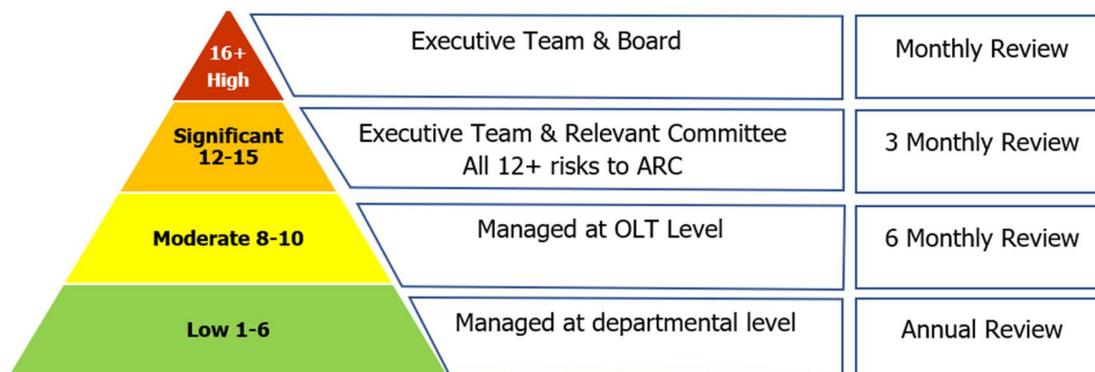
3.6 The risk is assessed by considering the following dimensions:
- Risk appetite (high, medium, medium/low, low)
- Impact of the risk (scale of 1-5, where 5 is the most significant)
- Likelihood of risk occurrence (scale of 1-5, where 5 is the most probable)
- Description of worst-case outcome, including a financial quantification if appropriate
- In addition, 'direction of travel' is also noted, whether we think that overall the impact of the risk has stayed static since previous review or is changing for better or worse.

Please refer to **Appendix A** for Risk Scoring Matrix which is a risk map diagram that depicts the relationship between impact and likelihood and the risk scored outcome of that relationship. **Appendix B** provides a guide for the scoring of risks by providing descriptors for the potential consequences and the likelihood of risk.

All risks are scored based on the above factors. Current or inherent mitigating factors are then considered to arrive at a 'mitigated risk score'. Once scored, risks are held, managed and reviewed as per the management chart below:

16+ High	Executive Team & Board	Monthly Review
Significant 12-15	Executive Team & Relevant Committee All 12+ risks to ARC	3 Monthly Review
Moderate 8-10	Managed at OLT Level	6 Monthly Review
Low 1-6	Managed at departmental level	Annual Review

The review dates are based on a minimum review frequency but may be reviewed more often if required.

3.7 All risks are held on the 'Vantage' risk management module and are assigned an owner (this may be a manager, OLT member or an Executive Lead), a named Executive Lead (if not owned by an Executive) and linked to one or more Strategic Risks.

3.8 The risk owner is responsible for the managed mitigation strategy. The key elements of the managed mitigation strategy are noted in Vantage. Each risk is assigned to a principle Committee of the Board, to where the risk is escalated should the risk score become 12 or higher.

3.9 Vantage will hold departmental operational risks and corporate risks within the same module, allowing for any high scoring risks to be escalated and de-escalated to the corporate register as required.

4. Monitor, review and communicate risk activities

4.1 The Board of Trustees is ultimately responsible for the system of risk management and internal control and through the Audit and Risk Committee reviews the effectiveness of this system. Every year the Board considers the nature and extent of the corporate and strategic risks that St Luke's engage with to achieve its strategic objectives. For each strategic risk, risk appetite is assessed to balance opportunities for business development and growth in areas of potentially higher risk, while maintaining reputation and reasonable levels of broad stakeholder support.

4.2 The Board Assurance Framework represents St Luke's key strategic risks and The Board will have sight of the Strategic Risks as part of the BAF and this will show a headline view of any risk movement within the organisation.

4.3 Trustees are required to report on the adequacy of the risk management framework under Charities SORP. As well as a risk systems adequacy statement, a description of each principal risk is published by trustees in the annual report.

4.4 Risk management is factored into business planning, performance management, audit and assurance, business continuity management and project management and monitoring. The Executive Team and Heads of Department commit to a culture where risks are considered and escalated as they arise and consider the risk profile of all new projects and activities before they are commenced.

5. Training Requirements
Local Vantage training, identification and management of risk for OLT and Executive Team.

6. Other related Policies / Procedures / Guidelines
Incident Management Policy
Health and Safety Policy
Business Continuity Policy
Complaints Policy.

7. References

Charities and Risk Management, UK Government Guidance CC26
https://www.gov.uk/government/publications/charities-and-risk-management-cc26/charities-and-risk-management-cc26 (Last accessed 21.08.25)

National Patient Safety Agency – A risk matrix for risk managers 2008.
https://nhgerm.wordpress.com/wp-content/uploads/2010/02/11-npsa_risk_matrix_for_risk_managers_v91.pdf (Last accessed 21.08.25)

8. Equality Impact Assessment

	Impact*	Advances equality	Eliminates discrimination	Fosters good relations
Race, nationality	Neutral			
Religion, belief and non-belief	Neutral			
Disability	Neutral			
Sex	Neutral			
Gender reassignment	Neutral			
Sexual orientation	Neutral			
Age	Neutral			
Pregnancy and maternity	Neutral			
Marriage and civil partnership	Neutral			
Human rights	Neutral			
Carers	Neutral			
Other groups	Neutral			

*Impact:

Positive: Will actively promote or improve equality of opportunity or address unfairness or tackle discrimination

Negative: Will have a negative or adverse impact which will cause disadvantage or exclusion

Neutral: No likely impact on any of the protected groups.

Appendix A – Risk Matrix

Risk Rating		Consequence				
		1 Neg/Min	**2** Minor	**3** Mod	**4** Major	**5** Severe
Likelihood	**5** Almost Certain	5	10	15	20	25
	4 Likely	4	8	12	16	20
	3 Possible	3	6	9	12	15
	2 Unlikely	2	4	6	8	10
	1 Rare	1	2	3	4	5
	Low		Moderate	Significant		High

Appendix B -Risk Consequence & Likelihood

Table of consequences					
Domain:	Consequence score and descriptor				
	1	**2**	**3**	**4**	**5**
	Minimal	**Minor**	**Moderate**	**Major**	**Severe**
Injury or harm Physical or Psychological	Minimal injury requiring no / minimal intervention or treatment No Time off work required	Minor injury or illness requiring intervention Requiring time off work < 4 days Increase in length of care by 1-3	Moderate injury requiring intervention Requiring time off work of 4-14 days Increase in length of care by 4-14 days RIDDOR / agency reportable incident	Major injury leading to long-term incapacity/disability Requiring time off work for >14 days	Incident leading to fatality Multiple permanent injuries or irreversible health effects
Quality of Patient Experience / Outcome	Unsatisfactory patient experience not directly related to the delivery of clinical care	Readily resolvable unsatisfactory patient experience directly related to clinical care.	Mismanagement of patient care with short term affects <7 days	Mismanagement of care with long term affects >7 days	Totally unsatisfactory patient outcome or experience including never events.
Statutory	Coroners verdict of natural causes, accidental death or open	Coroners verdict of misadventure Breech of statutory legislation	Police investigation Prosecution resulting in fine >£50K	Coroners verdict of neglect/system neglect	Coroners verdict of unlawful killing Criminal prosecution or imprisonment of a Director/Executive

	No or minimal impact of statutory guidance		Issue of statutory notice	Prosecution resulting in a fine >£500K	(Inc. Corporate Manslaughter)
Business / Finance & Service Continuity	Minor loss of non-critical service Financial loss of <£10K	Service loss in a number of non-critical areas <6 hours Financial loss £10-50K	Service loss of any critical area Service loss of non-critical areas >6 hours Financial loss £50-500K	Extended loss of essential service in more than one critical area Financial loss of £500k to £1m	Loss of multiple essential services in critical areas Financial loss of >£1m
Potential for patient complaint or Litigation / Claim	Unlikely to cause complaint, litigation or claim	Complaint possible Litigation unlikely Claim(s) <£10k	Complaint expected Litigation possible but not certain Claim(s) £10-100k	Multiple complaints / Ombudsmen inquiry Litigation expected Claim(s) £100-£1m	High profile complaint(s) with national interest Multiple claims or high value single claim. £1m+
Staffing and Competence	Short-term low staffing level that temporarily reduces patient care/service quality <1day Concerns about skill mix / competency	On-going low staffing level that reduces patient care/service quality Minor error(s) due to levels of competency (individual or team)	On-going problems with levels of staffing that result in late delivery of key objective/service Moderate error(s) due to levels of competency (individual or team)	Uncertain delivery of key objectives / service due to lack of staff Major error(s) due to levels of competency (individual or team)	Non-delivery of key objectives / service due to lack/loss of staff Critical error(s) due to levels of competency (individual or team)

Reputation or Adverse publicity	Rumours/loss of moral within the Trust Local media 1 day e.g. inside pages or limited report	Local media <7 days' coverage e.g. front page, headline Regulator concern	National Media <3 days' coverage Regulator action	National media >3 days' coverage Local MP concern Questions in the House	Full public enquiry Public investigation by regulator
Compliance Inspection / Audit	Non-significant / temporary lapses in compliance / targets	Minor non-compliance with standards / targets Minor recommendations from report	Significant non-compliance with standards/targets Challenging report	Low rating Enforcement action Critical report	Loss of accreditation / registration Prosecution Severely critical report

Table of likelihood					
Description:	1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
Frequency: (How often might it / does it occur)	This will probably never happen/recur Not expected to occur for years	Do not expect it to happen/recur but it is possible it may do so Expected to occur at least annually	Might happen or recur occasionally Expected to occur at least monthly	Will probably happen/recur, but it is not a persisting issue/circumstances Expected to occur at least weekly	Will undoubtedly happen/recur, possibly frequently Expected to occur at least daily
Probability:	Less than 10%	11 – 30%	31 – 70 %	71 - 90%	> 90%