RISK MANAGEMENT POLICY

Document configuration control

Policy Title	Risk Management Policy
Author/Job Title	Jonathan Sutton / CEO
Policy Version	Version 1.1
Status	Live
Reference and guidance	
Consultation Forum	Service Managers
Date of Consultation	27 Oct – 30 Jan 2016
Approving Body	Board of Trustee
Approval Date	10 April 2018
Review Date	1 April 2019
Last Amendment Date	17 May 2018
Amended By	Jonathan Sutton / CEO
Available on external website	No
Available on intranet	Yes
Standing Operating Procedures that reference this policy	Nil
Role responsible for this policy	CEO

Date of change	**Reason for change or amendment**	**Name of person and job title making change**	**Document version number**
24 Oct 2015	Creation of document	J Sutton CEO	DRAFT
25 Jan 2016	Final draft	J Sutton CEO	Final Draft
30 Jan 2016	Approved	J Sutton CEO	Version 1.0
17 May 2018	Update Probability and Impact levels	J Sutton CEO	Version 1.1

RISK MANAGEMENT POLICY

INTRODUCTION

1. This policy sets out the approach and commitment to the management of risk. It acknowledges that all businesses operate in an environment of opportunities and threats (risks) and introduces a framework and process to identify, assess, plan and implement risk management. This risk management process should enable a proactive risk management culture that is embedded throughout the organisation.

DEFINITION OF RISK

2. Risk is defined as '*an uncertain event or set of events that, should it occur, will have an effect on the achievement of objectives. A risk is measured by the combination of the probability of a perceived threat or opportunity*[1] *occurring and the magnitude of its impact on the objectives*'.

LEGISLATION AND REGULATION

3. The Charity (Accounts and Reports) Regulations 2008 states that Charities that are required by law to have their accounts audited must make a risk management statement in their trustees' annual report confirming that '...*the charity trustees have given consideration to the major risks to which the charity is exposed and satisfied themselves that systems or procedures are established in order to manage those risks*'. The statutory audit thresholds effective from 1 April 2009 are;

a. An income of £500,000 or more or
b. A gross income exceeding £250,000 with gross assets held exceeding £3.26 million.

RISK MANAGEMENT POLICY STATEMENT

4. The Board of Trustees of St Paul's takes responsibility and accountability for the management of risks. Discharging these responsibilities through the implementation of this policy will play a significant part to ensure that the organisation continues to meet and deliver its objectives.

5. The risk management policy provides an explanation of how risks will be identified, managed and determines the actions required to minimise (or exploit) the impact of these risks to the assets, reputation and financial viability of the organisation. It enables St Paul's to manage strategic decision-making, service delivery and to safeguard the interests of beneficiaries, the staff and other stakeholders.

[1] Risks can be a beneficial event (an opportunity) and the term 'upside risk' is relevant. Risks are more often considered as a negative event (or a threat) and the term 'downside risk' is relevant.

POLICY OBJECTIVES

6. The objectives of this policy are:

a. To adopt a strategic approach to risk management that encourages informed decision making to make the most of opportunities while managing threats.

b. To understand risk appetite, risk capacity and risk exposure and acknowledge that our approach to risks will be different depending on risk probability and impact.

c. To provide effective monitoring and intelligence on the risks facing the organization and to ensure that appropriate risk control measures are in place.

d. To ensure that the regulatory, legislative and best practice requirements in relation to risk management are met.

e. To protect our assets and the interests of our beneficiaries, donors, funders, employees and the general public.

f. To enhance the reputation of St Paul's by anticipating and responding well to risks.

RISK MANAGEMENT PRINCIPLES

7. The risk management principles adopted by St Paul's are set out below. The following principles should underpin all risk assessments and the implementation of risk management procedures:

a. Create and protect value. Risk management should create and protect value by helping St Paul's to achieve its organisational objectives.

b. Informs decision making. Risk management should inform all decision making processes, at all levels, within St Paul's.

c. Removes uncertainty. Risk management should remove uncertainty through being transparent, unambiguous and clearly communicated to all stakeholders.

d. Clear guidance. Risk management provides clear guidance to decision makers.

e. Enables judgements. It should enable systematic judgements of risk, in a timely and structured way.

f. Information quality. The information used in risk management should be the best quality available at the time.

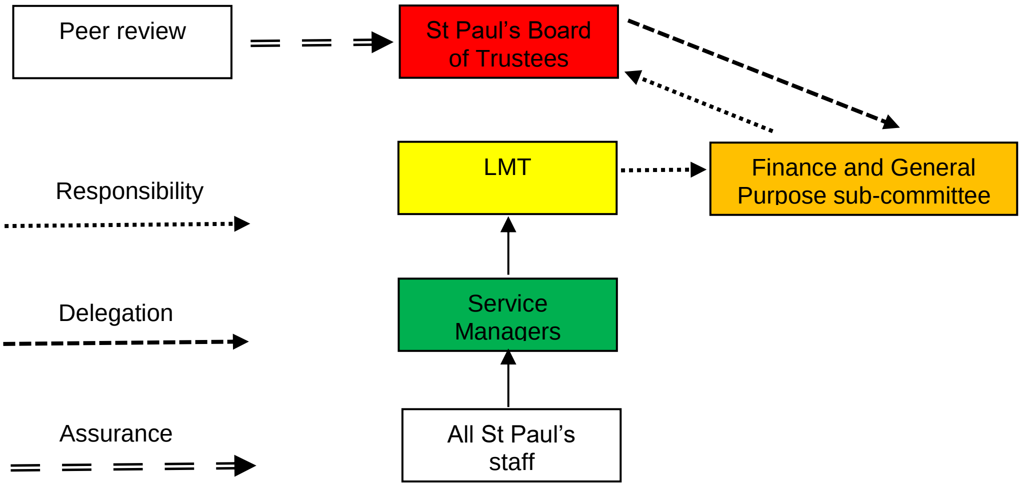
g. Tailored to context. Risk management should be tailored to the context of the risks faced by St Paul's.

h. Dynamic and responsive. Risk management is a continual process, regularly reviewed, anticipating or in response to change.

i. Facilitates improvement. Risk management should facilitate improvement across the whole organization.

j. Engages stakeholders. Risk management engages stakeholders in the identification, assessment and control of risks and also deals with the differing perceptions or risk.

Roles and responsibilities



8. St Paul's Board of Trustees. The Board will have overall responsibility for risk management. The Board will:

a. Set the tone and influence the culture of risk management for the organisation.
b. Approve risk management policy that sets the organisation-wide approach to risk management.
c. Ensure Board members have relevant risk management training so they can provide effective governance.
d. Determine the appropriate risk appetite and risk tolerance for the organisation.
e. Monitor the most significant risks to reduce the probability or impact and be satisfied that the less significant risks are being proactively managed
f. Ensure compliance with any statutory risk management arrangements.
g. Receive reports on individual very high or high risks as and when they arise and the mitigation measures that are put in place.

9. Finance and General Purpose Committee. The Finance and General Purpose Committee will have delegated responsibility for reporting, monitoring and reviewing risks in support of the Board of Trustees. The Finance and General Purpose Committee will work with the Leadership and Management Team to:

a. Recommend the Risk Management Policy to the St Paul's Board along with changes following peer review.
b. Gain assurance that the risk management arrangements are supported by an effective control environment
c. Review reports on the effectiveness of the systems for risk management, principally through annual Peer Review but also through visits and discussion with staff.
d. Receive quarterly reports on risks from Risk Registers from the Leadership and Management Team.

10. Leadership and Management Team**.** The Leadership and Management Team (LMT) will provide leadership of risk management throughout St Paul's. The LMT will:

a. Advise the Board on effective risk management and ensure that Board members receive relevant risk information
b. Take ownership of St Paul's risk registers and ensure that risks are owned and reviewed regularly
c. Ensure that all Board reports that support strategic or policy decisions include a risk assessment
d. Monitor the implementation of risk control measures to mitigate risk
e. Ensure that processes are in place to report any new or emerging risks, and to identify failures of existing controls
f. Ensure all staff are aware of the Risk Management policy and know how to identify, assess and report risks within their roles.

11. Service Managers

a. Regularly review risk registers.
b. Communicate with staff about current or emerging risks and how risks are identified and reported.
c. Communicate risks to higher authority that are above delegated threshold.

12. Risk response options. Risk response options are the standard actions that will be taken with all identified risks. The response options at St Paul's are;

a. Avoid This option makes an uncertain situation certain by removing the risk. It can often be achieved by removing the cause of a threat, or by implementing the cause of an opportunity.

b. Accept This option means that the organisation 'takes the chance' that the risk will occur with its full impact if it did. There is no change to the resident risk with the accept option but neither are there costs incurred now to manage the risk, or prepare to manage the risk in future.

c. Transfer is an option that aims to pass part of the risk to a third party. Insurance is a classic example where the insurer picks up the risk cost but the insured retains the impact. Cost of transference must be justified in terms of change to residual risk – *is the insurance premium worth paying*? Some elements of risk cannot be transferred but the organisation may choose to delegate the management of that risk to a third party.

d. Share. This is an option that is different in nature from the transfer response. It seeks for multiple parties, typically within a supply chain, to share the risk on a pain / gain share basis. Sharing risks is sometimes not possible, for example organisational reputation, but sharing does encourage collaboration.

e. Reduce (a threat) This option chooses definite action now to change the probability and/or the impact of the risk. The term mitigate is relevant when discussing reduction of a threat (i.e. making it less likely to occur or reducing the impact).

f. Enhance (an opportunity) Enhancing an opportunity is the reverse of reducing a threat, i.e. making it more likely the risk opportunity would occur / and or increasing the impact if it did. This option commits the organisation to costs for reduction or enhancement now therefore response cost must be justified in terms of the change to residual risk.

13. Risk appetite, risk capacity, risk exposure and risk tolerance. The Trustees will determine the level of appetite, understand organizational risk capacity and risk exposure.

a. Risk appetite. This is the amount of risk the organisation, or subset of, is willing to accept.

b. Risk capacity. The maximum amount of risk that an organisation, or subset, can bear. It is linked to reputation, capital assets and ability to raise funds. The organisation should not have a risk appetite that exceeds the risk capacity.

c. Risk exposure. The level of current risk borne at a point in time by the organisation. It is linked to risk capacity and risk appetite. Risk exposure should not be greater than risk capacity.

d. Risk tolerance. The threshold levels of risk exposure that, with appropriate approval, can be exceeded, but which when exceeded will trigger some form of response. For example reporting the situation to senior manager. A risk tolerance line might be drawn on the Risk Profile Summary.

14. **Risk tolerance thresholds.** The risk tolerance levels of risk exposure that, with appropriate approvals, can be accepted (lived with) without referring them to a higher authority.

Assessment of risk (Probability x Impact)	Action to be taken
A1, A2, A3, B1 and B2	Always managed at Board of Trustee level.
A4, B3, C1, C2,C3, D1,D2	Managed by the Finance and General Purpose sub-committee. Consider elevating these risks to Board of Trustees where probability or impact are worsening. Consider delegating if probability or impact are improving.
B4,C3,D3	Managed at Leadership Team. Consider elevating to Finance and General Purpose sub-committee where probability or impact judged to be worsening.
C4,D4	Managed by the service manager. Service manager may consider elevating to Leadership and Management Team where assurance is required, or if probability or impact is likely to worsen.

15. Procedure for escalation and delegation. This section describes the escalation procedure and delegation procedure to be adopted for organisation. The delegation procedure is how the Leadership and Management Team and service managers are advised of tolerance thresholds (see above) to which they are required to adhere.

16. In the event that a single risk or a group of risks exceed agreed threshold then the results should be escalated to a senior manager. The senior manager will then be responsible for either deciding on a course of action or escalating the information to a more senior level. Similarly it should be clear where a risk can be delegated to a lower level.

17. Risk Registers are the way to communicate risks that have been identified through the risk management process. It is necessary to complete or update a risk register when a risk is being escalated to a more senior level or transferred to another department.

18. Risk management process. The risk management process sets out an organisational approach that is to be followed. The process and the language in each step provide a common understanding across the organisation.

19. **Step 1: Identify the risks.** Goal of this step is to identify the risk to the activity or objectives with the aim of minimising threats while maximising opportunities.

a. Outputs from this step are;

i. Create a risk register.
ii. Early Warning Indicators for KPIs.

20. Risk registers. There are four risk registers maintained at St Paul's

a. Strategic Risk Register. This contains risks that have been assessed that may have a direct impact on the overall objectives of the organisation.

b. Service Risk Register. This contains risks that may impact on the achievement of service delivery or the delivery of specific services or projects. It equates to an operational Risk Register.

c. Building Risk Register. This contains risks that are specific to the buildings and to the maintenance of the buildings.

21. Service User Risk Register. Each Service User has a Risk Register.

22. For consistency, all of the risks are held on their respective registers hold the same level of information:

Risk Identifier	Risk impact	Risk Owner
Date risk identified	Pre-action risk	Risk actionee
Raised by	Risk Response option	Probability
Risk cause	Risk Action	Impact
Risk event	Action status	Proximity
Risk Identifier	Risk status	Risk Response
Action status	Risk status	

23. **Step 2: Assess and evaluate**. Goals of this step are to prioritise individual risks so that it is clear which risk are most important and most urgent <u>and</u> to understand the risk exposure faced by looking at net effects of the identified risks, when aggregated together.

a. Outputs from this step are;

i. Summary risk profile.
ii. Relationship and interdependencies.

Probability scale

Probability	Criteria	Likelihood
A Very likely	80 – 99%	Almost certainly will occur
B Likely	51 – 80%	More likely to occur than not
C Possible	10 – 50%	Fairly likely to occur
D Unlikely	1 – 10%	Unlikely to occur

Impact scale

Impact	Evaluation of impact	Cost or financial impact
1 Very High	Catastrophic impact that is possibly irreversible	Greater than £50k
2 High	Makes a significant and long lasting impact	£15k - £50k
3 Medium	Serious impact but not long lasting	£500 - £15k
4 Low	Some adverse impact	Under £500

24. **Step 3: Plan.** Goal of this step is to prepare specific management responses to the threats and opportunities identified ideally to remove or reduce the threats and to maximize the opportunities. Done well, the business and its staff are not taken by surprise if a risk materializes.

a. Risk owner
b. Risk actionee
c. Risk register (including risk responses and secondary risks)
d. Risk response plan

25. **Step 4: Implement.** Goal of this step is to ensure the planned risk management actions are implemented and monitored as to their effectiveness and corrective action is taken where responses do not match expectations. Outputs from this step are;

a. Monitoring is required to understand if responses are having the desired aim. Monitoring alone is a passive act so pro-active review of the threats or opportunities that contributed to the risk are also necessary.

b. Control is not a neutral action because it requires intervention. Controlling uses information from monitoring to take proactive action. To be effective, these actions must be economical, meaningful, appropriate, timely, simple and operational.

c. Update risk register with new risks, closed risks, revised and residual risks.

d. Reporting is necessary on a regular basis providing visibility of progress made.

Summary Risk Profile Template

Probability or risk happening	**A**	Very likely 80-99%	A4	A3	A2	A1
	B	Likely 51-80%	B4	B3	B2	B1
	C	Possible 10 – 50%	C4	C3	C2	C1
	D	Unlikely 1 – 10%	D4	D3	D2	D1
			Low	Medium	High	Very High
			4	**3**	**2**	**1**

Probability or risk happening	**A**	Very likely 80-99%	Moderate action required –mitigate to drive a route to green	Intensive action required – Manage through a LMT action plan	Intensive action required – Manage through a LMT action plan	Intensive action required – Managed by CEO (inform Trustees)
	B	Likely 51-80%	Minimal action required – monitor and accept where possible	Moderate action required –mitigate to drive a route to green	Intensive action required – Manage through a LMT action plan	Intensive action required – Manage through a LMT action plan
	C	Possible 10 – 50%	Minimal action required – monitor and accept where possible	Minimal action required –mitigate to drive a route to green	Moderate action required –mitigate to drive a route to green	Moderate action required –mitigate to drive a route to green
	D	Unlikely 1 – 10%	No action required – close the risk	Minimal action required – monitor and drive a route to green	Moderate action required –mitigate to drive a route to green	Moderate action required –mitigate to drive a route to green
			Low	Medium	High	Very High
			4	**3**	**2**	**1**

Risk Management Action

31. Communicate. Communication is not a distinct step in the process but an activity that is carried out throughout the whole process. A number of aspects of communication should be recognised and addressed if risk management is to be effective;

32. An organisation's exposure to risk is never static and effective and timely communication is central to the identification of new threats and opportunities or changes to existing risks.

33. Implementation or risk management is dependent on participation, and participation in turn, is dependent of communication. It is important for management to engage with staff across the organisation to ensure that;

a. Everyone understand the risk management policy, risk process and risk strategy relevant to their role.

b. Everyone understands how the organisation's risk capacity and risk appetite is expressed by risk tolerances for the work in question.

c. Everyone understands the benefits of effective risk management and the potential implications if it is not done or is done badly.

d. Each level of management, including the Board of Trustees, actively seeks and received appropriate and regular assurance about the management of risk within their control.

34. Effective communication provides assurance that risk is being managed with the expressed risk appetite and that risks exceeding tolerance levels are being escalated to pre-agree levels of management.

35. There is no misunderstanding over the respective risk priorities with and across each part of the organisation. This will help management avoid being diverted from the most significant risks and will enable appropriate levels of control to be applied.

36. Annual review. The risk management policy will be reviewed annually and when it is apparent that the policy is not working as well as expected. Following any review a risk improvement plan should be created and updated to drive and monitor the required improvement.

37. Assurance and peer review. Assurance is an essential element for Trustees. Peer review of risk management policy will be undertaken on an annual basis.

38. Budget. An annual budget of £250 for Risk Management training.

Glossary

39. Risk appetite is defined as '*the amount of risk the organisation, or subset of it, is willing to accept*".

40. Risk capacity is defined as "*the maximum amount of risk that an organisation or subset of it, can bear, linked to factors such as its reputation, capital assets and ability to raise additional funds*".

41. Risk exposure is defined as "*the extent of risk borne by the organisation at that time*"