

SPS Risk Management Policy

OUR APPROACH TO MANAGING RISK



1. Why we need to have this policy

The Trustees - Executive and Council - of Southgate Progressive Synagogue formally acknowledge their commitment to adopt and maintain best practice in the identification, evaluation, and effective control of risks to ensure they are managed to an acceptable level. In addition to threats, risks include loss of opportunities.

It is recognised that some risks will always exist and can never be eliminated. The underlying approach and specific procedures for the implementation of this policy - making every reasonable effort to manage risk appropriately by minimising the adverse effects of risk and maximising potential opportunities - are set out below.

2. Key messages

The following key principles outline the Southgate Progressive Synagogue (hereafter referred to as SPS) approach to risk management and internal control:

Southgate Progressive Synagogue (hereafter referred to as SPS) Council has ultimate responsibility for overseeing risk management within the organisation, which is a registered charity. Internal control is the primary approach - this means our policies and procedures forming the framework in which SPS operates.

The SPS Executive is responsible for supporting the SPS Council in risk management activities and coordinating risk management processes, ensuring appropriate reports and data are available to support the SPS Council with their decisions.

All SPS employees, volunteers and members are responsible for encouraging good risk management practice within their aspects of being a part of the SPS community.

Risks will be identified by the Trustees, employees, and volunteers, and monitored on a regular basis.

3. Role of the SPS Council (effectively a charity board of trustees)

SPS Council has a fundamental role to play in the management of risk.

With support from the SPS Executive they will set the tone and influence the culture of risk management within SPS.

This includes:

- Communicating the SPS approach to risk.
- Determining what types of risk are acceptable and which are not.

- Determining the appropriate risk tolerance or level of exposure for SPS.
- Approving major decisions affecting risk profile or exposure.
- Identifying risks and monitoring the management of significant risks to reduce the likelihood of adverse results.
- Satisfying themselves that the less severe risks are being managed, with the appropriate controls in place and that the controls are working effectively.
- Regularly reviewing the SPS approach to risk management and approving changes or improvements to key elements of the processes and procedures.

4. Involvement of SPS employees and volunteers

- Identifying and correctly evaluating the main risks faced by SPS for consideration by SPS Council.
- Implementing policies on risk management and internal control.
- Ensuring key risks are being managed appropriately using the agreed controls and responses to them and that the risk management framework and internal control systems are operating effectively.
- Providing adequate information in a timely manner to SPS Council on the status of risks and controls.
- Undertaking, together with SPS Council, a regular review of the effectiveness of the system.

5. Risk management as part of the system of internal control (SPS policies and procedures)

Any system of internal control incorporates risk management. This system encompasses several elements that together facilitate an effective and efficient operation; enabling SPS to respond to a variety of governance, operational, financial, external and compliance risks. These elements include the policies that underpin the internal control process which have been approved by SPS Council and are implemented and communicated to SPS employees, volunteers, and members. Written procedures support the policies where appropriate.

6. Reporting

Comprehensive reporting via a risk register is designed to monitor key risks and their controls. Decisions to rectify problems are made at regular SPS Council meetings.

7. Operational planning and budgeting

The operational planning and budgeting process is used to set objectives, agree action plans, and allocate resources. progress towards meeting these objectives being monitored regularly.

8. External audits and third parties

External audits, when and where appropriate, provide feedback to SPS Council on the operation of the internal controls, reviewed as part of regular auditing. (e.g. Fire Risk Assessment).

From time to time, the use of external agencies may be necessary in areas such as fire and safety, as well of course as the annual financial audit of the SPS accounts. The use of such external agencies for consulting and reporting can increase the reliability of the internal control system.

9. Risk management process

SPS operates the following risk management process:

- Review of the previous year's risk management systems.
- A 'risk identification' exercise to design the risk register.
- Evaluation of identified risks using risk assessment (see Appendices).
- Managing risks by applying risk management techniques.
- Recording and monitoring risks using the risk register.
- Assigning responsibility for risks appropriately.

Risk identification is not just an annual / regular interval process - SPS Council, employees and members are encouraged to report on risk, update risk registers and carry out any necessary assessments throughout the year.

10. Risk Assessment

Risk assessment helps protect the public coming into our place of worship as well as ensuring we work within the law. It helps you focus on the risks that really matter - the ones that could possibly cause genuine harm.

A risk assessment is simply a careful examination of all aspects of anything in our synagogue buildings that could cause harm to people, so that we can decide whether we have taken enough precautions or if we need do more to prevent harm. The law does not expect any establishment to totally eradicate risk, but to protect people as far as is reasonably possible.

When thinking about risk assessments, it is important to remember:

- a hazard can be anything that has the potential to cause harm
- a risk is the chance, high or low, that somebody may be harmed by the hazard

When carrying out risk assessments, it may be helpful to divide SPS into different activities or areas and deal with each of these separately. This will be less daunting than trying to carry out a risk assessment for the whole site, buildings, and grounds.

10.1 The five steps to assessing risk:

Step 1: Identifying hazards and those at risk - what has the potential to cause injury or ill-health?

Step 2: Decide who might be harmed and how.

Step 3: Evaluate the risks and decide on precautions.

Step 4: Record the findings and implement them.

Step 5: Review our risk assessment and update as necessary.

11. Regular review of effectiveness

SPS Council, with support from the SPS Executive, is responsible for reviewing the effectiveness of internal control through findings based on the information provided by employees, volunteers, and members. Its approach is outlined below.

For each major risk identified, SPS Council will:

- Review the previous year and examine SPS's track record on managing and internally controlling the risk.
- Consider the internal and external risk profile for the coming year and consider if the current controls are likely to be effective.

In making these decisions, SPS Council will consider the following aspects.

11.1. Control Environment:

- SPS's objectives and its financial and non-financial targets.
- The organisational structure and calibre of the staff.
- The culture, approach, and resources for managing risk.
- Appropriate delegation of authority.
- Public reporting, if relevant.

11.2. On-going Identification and Evaluation of Significant Risks:

- Timely identification and assessment of major risks.
- Prioritisation of risks and allocation of resources to address areas of high exposure.

11.3. Information and Communication:

- Quality and timeliness of information on newly identified risks.
- The time it takes for breakdowns in control to be recognised and/or new risks to be identified / recognised.

11.4. Monitoring and Corrective Action:

- The ability of SPS to learn from its problems.
- The commitment and speed with which corrective actions are implemented.

12. Internal control

The risk of falling short of the above stated standards is mitigated as far as possible by ensuring that appropriate policies and operational practices are adopted in each key area and that Trustees, staff and volunteers are adequately experienced and trained to manage this. Where necessary, external advice will be sought to supplement internal expertise.

13. Policy revision

This policy will be reviewed every three years and amended as necessary, or earlier in accordance with any forthcoming new legislation.

All employees and volunteers should pass suggestions or recommendations for the revision of any aspect of this policy through the SPS Honorary Secretary to the SPS Executive and Council.

Date: 1st November 2023

Review Date: November 2026

Signature: *Mark Howard Shaw*

Printed Name: Mark H Shaw

SPS Chair on behalf of SPS Executive and Council

Appendix 1

Typical Risk Categories

1. Physical / Environmental (e.g. buildings, maintenance, health & safety, etc.)
2. Financial
3. Security / Safety (e.g. fire, terrorism [- on which advice will be taken from the CST / local Police / Government], etc.)
4. Legal / Political (legislation, employment issues, etc.)
5. IT (technology and software systems)
6. Religious / Educational / Pastoral (services, pupil and member support, outreach, etc.)
7. Governance (management and internal policies)
8. Competitive / Strategic / Reputational / Publicity
9. Synagogue / SPS specific

Appendix 2

Risk Factor Assessment and Matrix Guidance on the Definition of Likelihood and Impact

Likelihood

5- Very High

There is little doubt that it will happen soon
(Potential of it occurring several times within a year; Has already happened)

4- High

Strong chance it will happen in the next year
(Chance it could occur more than once; some history of occurrence)

3 - Significant

50/50 chance this will happen in the next year
(Chance it could occur over the next 2-3 years)

2- Low

Not expected to happen in the next year
(Not likely to occur; has not occurred in past 3 years)

1- Very Low

Almost impossible
(Has not occurred in the past)

Impact

5 - Major

Loss of operations for more than a week; severe injuries or loss of life; gross failure to meet national / professional standards; major long-term consequences; extensive coverage in press; major financial loss that threatens existence

4 - Significant

Loss of operations for up to a week; severe injuries; severe financial loss (requires use of reserves) with impact on operations; damage to reputation, local press coverage

3 - Moderate

Some disruption to operations (up to 48 hours); short term illness / injuries; some damage to reputation; financial loss than can be managed within revenue budget

2 - Minor

Limited short-term disruption to operations (within a business day); minor injuries / illness; small financial loss

1 - Negligible

Not a noticeable effect on the organisation; no injuries; no damage to reputation, financial impact is nil or negligible

Risk Matrix

LIKELIHOOD	5 Very High	5	10	15	20	25
	4 High	4	8	12	16	20
	3 Significant	3	6	9	12	15
	2 Low	2	4	6	8	10
	1 Very Low	1	2	3	4	5
		1 Negligible	2 Minor	3 Moderate	4 Significant	5 Major
		IMPACT				

	Negligible Risk
	Minor Risk
	Moderate Risk
	Major Risk

Appendix 3

Risk Register Template

Headings should include:

- Risk reference number
- Risk category / type (from Appendix 1)
- Strategy / policy area (e.g. Health & Safety, Finance, etc.)
- Description of actual risk
- Person(s) responsible (if relevant - e.g. Caretaker, Head of Security, etc.)
- Cause and effects
- Risk matrix score and categorisation of this risk (e.g. '10 - Moderate risk')
- Existing controls
- Actions required / actions taken
- Risk matrix score and categorisation after action(s) taken (e.g. '2 - Negligible risk')
- Risk tolerance level (e.g. we can live with this / we will need to do more)
- Date
- Review date (if any required)