Finchley Progressive Synagogue

Risk Management Policy

1. Why we need to have this policy

The Board of Trustees (Council) of Finchley Progressive Synagogue (FPS) 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 but are not limited to, loss of opportunities, financial and other loss, and damage of reputation.

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 FPS approach to risk management and internal control:

Council has ultimate responsibility for overseeing risk management within the organisation, a registered charity.

Internal control is the primary approach – as such, our policies and procedures form the framework in which FPS operates.

The Executive is responsible for supporting the Council in undertaking risk management activities and coordinating risk management processes, ensuring appropriate reports and data are available to support Council with their decisions. All FPS employees, volunteers and members are responsible for encouraging good risk management practice within their aspects of being a part of the FPS community.

Risks will be identified by Council, employees, and volunteers, and are monitored on a regular basis.

3. Role of Council

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

This includes:

• Communicating FPS's approach to risk.

• Determining which types of risk are acceptable and which are not.

• Determining the appropriate risk appetite, risk tolerance or level of exposure.

• 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.

• Ensuring any serious or high-level risk is escalated to the appropriate level to assess and deal with the risk correctly, in order to minimise exposure.

• Regularly reviewing the FPS approach to risk management and approving changes or improvements to key elements of the processes and procedures.

4. Involvement of FPS employees and volunteers

• Identifying and correctly evaluating the main risks faced by FPS for consideration by Council.

• Implementing appropriate 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. In the case of inadequate systems reporting them to Council or informing a person who can inform Council.

• Providing adequate information in a timely manner to Council on the status of risks and controls.

• Undertaking, together with Council, a regular review of the effectiveness of the system.

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

The system of internal control incorporates risk management.

This system encompasses several elements that together facilitate an effective and efficient operation; enabling FPS 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 Council and are implemented and communicated to FPS employees, volunteers, and members.

Written procedures support the policies where appropriate.

6. Reporting

Comprehensive reporting via the Risk Register is designed to monitor key risks and their controls. Decisions to rectify problems are made at regular 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 is monitored regularly.

8. External audits and third parties

External audits, when appropriate, provide feedback to 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 for areas requiring accredited expertise, such as fire and safety and financial matters.

The use of such external agencies for consulting and reporting can increase the reliability of the internal control system. All third parties will be appropriately qualified and accredited.

9. Risk management process

FPS operates the following risk management process:

- Review of the previous year's risk management systems.
- Identify new risks and update 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.
- Assessing progress and status of identified risks.

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

10. Risk Assessment

Risk assessment helps protect the public coming into our premises as well as ensuring we work within the law. It helps 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, in order to allow us to decide whether we have taken enough precautions or if we need to do more.

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 with 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 can be helpful to divide FPS into different activities or areas and assess with each of these separately.

10.1 The five steps to assessing risk:

Step 1: Identifying hazards and those at risk.

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

Council, with support from the 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, Council will:

• Review the previous year and examine FPS'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, Council will consider the following aspects.

11.1. Control Environment:

• FPS'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 FPS 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 Council, staff and volunteers are adequately experienced and trained to manage this. Where necessary, external advice will be sought.

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 FPS Honorary Secretary to the FPS Chair.

Beverley Kafka

Chair

Ratified: May 2026

Review date: May 2027

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, safeguarding etc.)

7. Governance (management and internal policies)

8. Competitive/Strategic/Reputational/Publicity

9. Synagogue/FPS specific

Example Risk Tolerance Level

Very Low Risk (Acceptable)

- Definition: We can live with this risk.
- Description: Minimal impact and/or unlikely to occur.
- Action: No immediate action required other than routine monitoring.

Low Risk (Tolerable)

- Definition: Acceptable with awareness.
- Description: Minor impact or low likelihood; unlikely to disrupt operations significantly.
- Action: Monitor and manage through normal procedures.

Moderate Risk (Manageable)

- Definition: Needs attention.

- Description: Noticeable impact if it occurs; moderate likelihood.
- Action: Implement controls to reduce risk within a reasonable timeframe.

High Risk (Undesirable)

- Definition: Not acceptable without mitigation.
- Description: Significant impact and/or high likelihood; could seriously affect objectives.
- Action: Prompt action required to reduce, transfer, or avoid the risk.

Extreme Risk (Intolerable)

- Definition: Urgent action required to avoid a catastrophic event.
- Description: Severe impact with high likelihood; threatens survival, safety, or compliance.
- Action: Immediate action required; activity should be stopped or not started until risk is reduced.

Appendix 2

Risk Factor Assessment and Matrix

Likelihood	
5 – Very High	There is very little doubt that it will happen soon (Potential of it occurring several times within a year; Has already happened).
4 – High	There is a strong chance it will happen in the next year (Chance it could occur more than once; some history of occurrence)
3 – Significant	There is a 50/50 chance it will happen in the next year (Chance it could occur over the next 2-3 years)
2 – Low	It is not expected to happen in the next year (Not likely to occur; has not occurred in past 3 years)
1 – Very Low	It is 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. Catastrophic.
4 – Significant	Loss of operations for up to a week; severe injuries; severe financial loss 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

Risk = Likelihood x Impact

Likelihood	Impact 1 Negligible	2 Minor	3 Moderate	4 Significant	5 Major
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

1–5 → Low risk

6–10 → Medium risk

11–15 → Significant risk

16–25 → High / Critical 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
- 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.