RISK MANAGEMENT POLICY AND PROCEDURES

Policy Statement

KidsAid is committed to a proactive and structured approach to risk management to safeguard its mission, assets, people, beneficiaries, and reputation. Effective risk management is integral to our governance, strategic planning, and day-to-day operations.

The Board of Trustees has a legal duty to manage risk appropriately and to protect the charity's resources and those it serves. This policy supports Trustees in fulfilling that duty by providing a clear and consistent framework for identifying, assessing, managing, and monitoring risk across all levels of the organisation.

It ensures that risk-taking is aligned with our values, legal obligations, and strategic priorities, and that both the Board and senior leadership are equipped to make informed decisions within a defined risk appetite.

We recognise that not all risks can be eliminated and that some level of risk is inherent in delivering impact. Therefore, we aim to:

- Promote a culture of awareness, accountability, and responsiveness to risk.
- Support informed decision-making through clear roles and escalation pathways.
- Embed risk considerations into planning, performance, and resource allocation.
- Ensure compliance with legal, regulatory, and sector-specific expectations, including guidance from the Charity Commission and other relevant bodies.

Risk oversight is a shared responsibility involving the Board of Trustees, its subcommittees, the CEO, and the Senior Leadership Team.

The Risk Register and supporting processes ensure that significant and emerging risks are actively monitored, reviewed, and addressed with appropriate mitigation strategies.

Introduction

This Risk Management Policy outlines the principles, responsibilities, and processes that guide how KidsAid identifies, assesses, mitigates, monitors, and reports risk. It supports our ability to meet legal, ethical, and strategic obligations by embedding risk management into decision-making at all levels.

The policy ensures that risk is managed consistently, transparently, and proportionately across the organisation. It helps us remain resilient in a dynamic environment, safeguard our beneficiaries and stakeholders, and promote long-term sustainability.

Scope

This policy applies to all trustees, senior leaders, managers, and staff at KidsAid. It encompasses all categories of risk relevant to the organisation's operations and strategic objectives, including but not limited to:

- **External:** Societal, political, and economic risks.
- **Financial:** Risks related to income, fraud, and budgeting.
- **Governance:** Risks concerning board effectiveness and legal compliance.
- **Operational:** Risks arising from internal processes, personnel, and systems.
- **Reputational:** Risks affecting stakeholder trust and public perception.
- **Regulatory and Compliance:** Risks associated with data protection, clinical practice, safeguarding, and ensuring adherence to legal, regulatory, and sector-specific requirements, including guidance from the Charity Commission and other relevant bodies.
- **Strategic:** Risks impacting mission alignment and strategic priorities.

These categories represent the broad areas in which risks may arise and provide a framework for identifying and managing risk across the organisation.

Risk Management Framework

Risk management is embedded within KidsAid's governance and is integral to our planning and performance processes. The Board and Senior Leadership Team provide oversight, ensuring significant risks are effectively managed and that risk information informs strategic and operational decisions. All staff are responsible for identifying and managing risks within their areas of control.

The Risk Management Cycle

Our risk management process is continuous and comprises the following key stages:

- **Identification:** Risks are identified through incident analysis, strategic reviews, and environmental scanning. Both current and emerging risks are considered.

- **Assessment:** Risks are evaluated by likelihood and impact, measured against our risk appetite and tolerance to prioritise resources on the most critical risks.
- **Mitigation:** Controls and response strategies are developed and applied, which may include risk avoidance, reduction, transfer, or acceptance, depending on the risk and our appetite.
- **Monitoring:** Risks and controls are continuously monitored through management meetings, subcommittees, and oversight by the Quality and Accreditation Subcommittee to ensure they remain effective and responsive to change.
- **Review:** Risk assessments and mitigation measures are periodically reviewed and updated to reflect evolving internal and external conditions. Lessons learned from incidents are integrated to enhance organisational resilience.

Use of the Risk Register

The Risk Register is a central element of the Risk Management Framework. It is a dynamic, living document that records all identified risks, their current status, assigned owners, mitigation actions, and review schedules. The register is regularly updated and accessible to all trustees and staff, promoting transparency, accountability, and coordinated management of risk across the organisation.

Strategic and Operational Integration

Risk management is fully integrated into key organisational processes, including:

- **Strategic Planning:** Risks are considered during the development and review of strategic objectives to ensure alignment with the organisation's risk appetite.
- **Project Management:** Risk assessments are embedded within project initiation and execution to identify and manage project-specific risks promptly.
- **Decision-Making:** Risk analysis supports significant decisions, enabling a balanced evaluation of opportunities and threats.

Risk Appetite

Our risk appetite defines the level and nature of risk the organisation is prepared to accept in pursuit of its objectives. It provides a framework for assessing risk tolerance and supports consistent decision-making throughout the organisation. The Quality and Accreditation Subcommittee regularly reviews the risk appetite and ratings on behalf of the Board to ensure it remains aligned with our strategic priorities, external environment, and stakeholder expectations.

Roles and Responsibilities

The following outlines the key roles and the associated responsibilities for ensuring that risk is identified, assessed, and managed consistently across the organisation.

Board of Trustees

- Hold ultimate responsibility for risk management, ensuring the charity operates within acceptable risk levels and remains resilient in fulfilling its mission.
- Provide strategic oversight of risk management.
- Approve and review the Risk Management Policy.
- Sets the organisation's risk appetite.
- Delegate ongoing risk oversight to the Quality and Accreditation Subcommittee.
- Respond to risks escalated by the Quality and Accreditation Subcommittee to the Board.
- Review the Risk Register once a year, focusing on strategic and high-impact risks.
- Ensure adequate resources, systems, and structures are in place for effective risk management.
- Promote a risk-aware culture and transparent risk reporting.

Quality and Accreditation Subcommittee

- Support the Board by providing focused oversight and assurance over risk management processes.
- Review the effectiveness of the risk management framework, internal controls, and compliance.
- Monitor the status of key risks and the effectiveness of mitigation actions as recorded in the Risk Register.
- Assess reports that relate to risk, compliance, or control failures.
- Ensure risk is considered in financial planning, safeguarding, compliance, and fundraising activities.
- Recommend updates to the Risk Management Policy and framework as needed.
- Escalate critical risk issues to the Board with recommendations for action.

CEO

- Implement the risk management framework and ensure risk considerations are integrated into the charity's strategic and operational management.
- Champion a culture of risk awareness and accountability throughout the organisation.
- Ensure that risk management practices are embedded in day-to-day operations, project planning, and decision-making.
- Lead the development and maintenance of the Risk Register.
- Report the status of escalated risks to the Quality and Accreditation Subcommittee.
- Ensure appropriate guidance is provided to staff on risk management.

Senior Leadership Team

- Identify and assess risks within their areas of responsibility and ensure risks are logged and regularly updated in the Risk Register.
- Develop and implement appropriate controls and mitigation strategies for operational and project risks.
- Monitor the effectiveness of risk controls and escalate significant risks or control failures to the CEO.
- Ensure staff within their teams are aware of key risks and are trained to respond appropriately.

All Staff and Volunteers

- Understand the risks associated with their roles and activities.
- Comply with the charity's policies, procedures, and controls designed to manage risk.
- Promptly report new or emerging risks, incidents, or near misses to their line manager.
- Participate in relevant training and risk awareness sessions.

Risk Identification and Assessment

Risks are identified through a variety of methods, including but not limited to:

- Strategic and operational planning sessions.
- Board, subcommittee and team meetings.
- Incident reporting and lessons learned.
- Regulatory changes and sector developments.
- Internal audits and external reviews.
- Ongoing project and programme assessments.

All staff and volunteers are encouraged to identify potential risks relevant to their areas of work. The Senior Leadership Team are responsible for reviewing and escalating these risks where appropriate.

New risks may be added to the Risk Register:

- During scheduled reviews of existing risks.
- When identified during project planning or delivery.
- In response to emerging threats or incidents.
- At the request of a trustee, subcommittee or CEO.

Each new risk must be clearly described, with details on the source of the risk, potential consequences, and any existing controls in place.

Inherent and Residual Risk

Each identified risk is assessed at two levels:

- **Inherent Risk:** The level of risk before any controls or mitigation strategies are applied. This reflects the raw exposure of the organisation to the risk.
- **Residual Risk:** The level of risk after existing controls and mitigation measures are considered. This reflects the actual, current level of exposure, and is used to determine whether further action is required.

Both scores are recorded in the Risk Register.

Risk Scoring Criteria

Risks are assessed based on two key factors:

- Likelihood: The probability that the risk will occur.
- Impact: The potential consequence if the risk materialises.

Each factor is scored on a five-point scale, with defined criteria to ensure consistency across the organisation.

Likelihood Scale

Score	Descriptor	Description
1	Rare	Unlikely to occur except in exceptional circumstances
2	Unlikely	Could occur but not expected in the near future
3	Possible	May occur occasionally or under specific conditions
4	Likely	Will probably occur in many circumstances
5	Certain	Expected to occur frequently or imminently

Impact Scale

Score	Descriptor	Description
1	Insignificant	Minimal or no impact.
2	Minor	Limited impact; easily manageable.
3	Moderate	Noticeable impact; may require additional resources or time.
4	Significant	Significant impact on service delivery, finances or reputation.
5	Major	Critical impact: threatens sustainability or causes major harm.

Risk Matrix and Risk Rating

The risk rating is determined by multiplying the likelihood and impact scores using a 5 x 5 risk matrix. This generates a risk score from 1 (lowest) to 25 (highest), which is used to prioritise risks for management attention.

Risk Matrix

Likelihood ↓ / Impact →	1	2	3	4	5
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

Risk Ratings

- 1–8 (Low): Acceptable risk; through routine controls; review regularly.
- 9–16 (Moderate): Requires specific risk mitigation and/or regular review.
- 20–25 (High/Critical): Immediate action required; senior-level oversight.

Both inherent and residual scores are recorded using the matrix, and actions are prioritised based on the residual risk rating.

Documentation and Review

The CEO is responsible for documenting all identified risks in the Risk Register, which includes the following information:

- Description of the risk and its potential impact.
- Inherent and residual risk scores.
- Existing controls and their effectiveness.
- Risk owners (individuals responsible for managing the risk).
- Mitigation actions and timeframes.
- Review schedule.

Risk Appetite and Tolerance

The risk appetite provides a framework for:

- Ensuring consistency in how risks are evaluated and managed.
- Supporting effective and transparent decision-making.
- Determining when risks should be escalated to senior management or the Board.
- Aligning risk-taking with the organisation's values, obligations, and strategic ambitions.

The Board sets and reviews the charity's risk appetite annually, considering internal capabilities, legal and regulatory obligations, and the external environment in which the charity operates. Risk tolerance sets thresholds for when risk must be escalated to the Quality and Accreditation Subcommittee.

Organisation-Wide Risk Appetite Statement

As a charity, our overarching risk appetite is moderate. We are willing to accept some measured risk where it supports innovation, service improvement, and long-term sustainability, but we maintain a cautious approach in areas where failure would seriously impact our beneficiaries, compliance obligations, reputation, or financial stability.

Risk Appetite by Category

We recognise that risk appetite varies across different areas of the organisation's activities:

Risk Category	Appetite Risk Level	Description
Safeguarding	Low	We have no tolerance for internal risks that could endanger the welfare or safety of beneficiaries, staff, or volunteers.
Compliance & Legal	Low	We maintain a very low appetite for breaches of law, regulation, or key policies (e.g. GDPR, charity law).
Reputation	Low to Moderate	We actively protect our reputation and stakeholder trust but may accept minor reputational risks to advance our mission.
Financial	Moderate	We accept that some financial risk is unavoidable in a constrained environment and will tolerate it where it supports strategic growth or efficiency, with strong oversight and mitigation.
Operational	Moderate	We are open to moderate operational risks that support service delivery or organisational improvement, provided they are managed effectively.
Innovation & Growth	High	We have a high appetite for calculated risks in innovation, new projects, and service models that offer significant social impact, provided risks are understood and appropriately managed.
IT & Cybersecurity	Low to Moderate	We are cautious in our approach to digital and cybersecurity risks, recognising their potential to disrupt operations and compromise data.

Risk Tolerance and Escalation Triggers

Risk tolerance sets thresholds for when risk must be escalated or reassessed. Where the residual risk rating exceeds the defined appetite for that category, it must be escalated to the CEO for review by the Quality and Accreditation Subcommittee.

Escalation Guidance

- Risks that exceed the defined appetite, such as safeguarding risks rated Moderate or higher, must be escalated to the CEO immediately.
- All high residual risks, irrespective of category, are reported by the CEO to the Quality and Accreditation Subcommittee. Minutes are circulated to the Board for full transparency.
- Emerging risks or significant changes in likelihood or impact must prompt a re-assessment and, if necessary, an update to the Risk Register.

Use in Decision-Making

Risk appetite informs decisions across key areas:

- Strategic choices, including launching new programmes or entering partnerships.
- Investment decisions, such as adopting new technologies or funding innovation.
- Operational planning, including balancing risk and opportunity in service delivery.
- Governance and oversight, through risk prioritisation and Board reporting.

By aligning decisions with our defined risk appetite, we ensure a balance between delivering our mission and exercising responsible stewardship of our resources, reputation, and duty of care.

Risk Monitoring and Reporting

Risks are continuously monitored to:

- Track changes in likelihood, impact, or exposure.
- Ensure mitigation measures are implemented and remain effective.
- Identify emerging risks or control failures early.
- Support timely decision-making and escalation.

Risk owners are responsible for actively monitoring the risks assigned to them, including the status of control actions and any changes in the external or internal environment that may affect the risk.

Review Frequency

All risks are reviewed on a bi-monthly basis, except those rated as high, which are reviewed monthly as a priority. Major risks relating to safeguarding, compliance, financial controls, or reputation may be reviewed more frequently at the discretion of the Board.

Internal Reporting Structure

Risk reporting follows a clear hierarchy to ensure transparency, accountability, and effective oversight:

- **Operational Teams:** Identify and report changes in risk or incidents to their line managers.
- **Senior Leadership Team:** Reviews operational and strategic risks at monthly management meetings. Risks requiring escalation are documented and flagged by the CEO.
- **CEO:** Oversees the risk management process, ensures timely updates to the Risk Register, and escalates key risks to the Quality and Accreditation Subcommittee.
- **Quality and Accreditation Subcommittee**: Reviews escalated risks and mitigation actions on a bi-monthly basis, or sooner in response to serious incidents. Provides assurance to the Board on risk oversight.
- **Board of Trustees**: Reviews risk reports submitted by the Quality and Accreditation Subcommittee and provides strategic direction based on risk insights. Annually reviews the Risk Management Policy, the full Risk Register, and the internal reporting structure.

Escalation and Incident Response

Any serious incidents, breaches of controls, or risks exceeding the organisation's risk appetite must be escalated immediately according to established escalation procedures. This includes:

- Significant safeguarding concerns.
- Regulatory compliance breaches.
- Major financial risks or fraud indicators.
- Critical reputational issues.

Where required, incidents may also be reported to the Charity Commission or other relevant regulatory authorities, in line with statutory obligations.

Review and Continuous Improvement

Risk management is not a one-off exercise but a dynamic, ongoing process that must evolve with the organisation's activities, environment, and strategic direction.

KidsAid is committed to regularly reviewing and improving its risk management practices to ensure they remain effective, proportionate, and aligned with best practice.

Regular Policy Review

The Risk Management Policy will be formally reviewed once a year, or in response to significant organisational changes, such as a shift in strategy, structure, or operating environment, or following a serious incident that highlights gaps in risk management.

Proposed updates to the policy are led by the Quality and Accreditation Subcommittee and must be approved by the Board of Trustees.

Ongoing Framework Evaluation

The effectiveness of the risk management framework will be evaluated through:

- Feedback from staff, volunteers, and trustees involved in risk processes.
- Analysis of control failures, incident trends, and lessons learned.
- Benchmarking against sector standards and regulatory expectations.

Improvements may include updating the risk assessment criteria, refining reporting formats, introducing new tools (e.g., dashboards or KRIs), or embedding risk more deeply into planning and performance processes.

Embedding a Culture of Learning

The charity promotes a culture where risks and lessons learned are openly discussed, and improvement is encouraged. This includes:

- Sharing findings from risk incidents or near-misses across teams.
- Encouraging staff and volunteers to identify and report emerging risks.
- Providing guidance as risk management practices evolve.
- Using outcomes from risk reviews to improve internal controls and decision-making.

Trustee and Staff Development

As part of continuous improvement, the charity will ensure:

- Trustees receive regular briefings on risk trends, policy updates, and regulatory expectations.
- Staff and volunteers receive appropriate guidance tailored to their roles and responsibilities in managing risk.