RISK ASSESSMENT & RISK MANAGEMENT POLICY
Neuro Gateway Support Network

1. Introduction and Statement of Commitment

Neuro Gateway Support Network is committed to maintaining a comprehensive and proactive approach to risk assessment and risk management in order to ensure the safe, lawful, and effective delivery of its services. The organisation recognises that risk is an inherent element of all activity, particularly when working with vulnerable individuals, sensitive information, and complex systems such as health and social care services.

The organisation acknowledges that unmanaged risk has the potential to result in harm to individuals, compromise safeguarding, breach legal obligations, and damage organisational reputation and sustainability. It is therefore essential that risk is identified, assessed, and managed in a structured and consistent manner.

This policy establishes the framework through which *Neuro Gateway Support Network* will identify potential risks, evaluate their likelihood and impact, implement appropriate control measures, and monitor outcomes. It reflects the organisation's commitment to safeguarding, accountability, and continuous improvement.

2. Purpose of the Policy

The purpose of this policy is to ensure that risk management is embedded within all aspects of the organisation's governance and operational practice. It provides a clear and consistent approach to identifying potential risks, assessing their significance, and implementing proportionate measures to mitigate them.

The policy also aims to support informed decision-making by ensuring that risks are understood and considered at both operational and strategic levels. It enables the organisation to anticipate potential challenges, respond effectively to incidents, and maintain a high standard of service delivery.

3. Scope and Application

This policy applies to all areas of activity undertaken by *Neuro Gateway Support Network*, including service delivery, governance, administration, communication, and partnership working.

It applies to all individuals acting on behalf of the organisation, including trustees, volunteers, and any individuals involved in supporting or representing the organisation.

Risk management considerations must be applied at all levels of activity, from individual casework and client interactions through to organisational planning and external engagement.

4. Definition and Nature of Risk

Within the context of this policy, risk is defined as the possibility that an event, action, or omission may occur which could have a negative impact on the organisation's ability to

achieve its objectives, or which may result in harm to individuals, breach of legal obligations, or damage to reputation.

Risks may arise from both internal and external factors and may vary in likelihood and severity. They may be immediate or emerging and may affect individuals, processes, systems, or the organisation as a whole.

The organisation recognises that risk cannot be entirely eliminated; however, it can be effectively managed through structured processes and informed judgement.

---

5. Categories of Risk

Neuro Gateway Support Network recognises that risks may arise across a range of areas and may overlap. Key categories of risk relevant to the organisation include operational risk, safeguarding risk, legal and regulatory risk, reputational risk, financial risk, and information governance risk.

Operational risks relate to the day-to-day functioning of the organisation and may include issues such as communication errors, insufficient resources, or process failures. Safeguarding risks relate to the safety and wellbeing of individuals accessing the service and may involve situations where individuals are at risk of abuse, neglect, or harm.

Legal and regulatory risks arise from potential failure to comply with applicable laws, including data protection legislation and safeguarding duties. Reputational risks relate to actions or events that may undermine public confidence in the organisation.

Financial risks involve the management of resources, funding stability, and financial sustainability. Information governance risks relate to the handling, storage, and protection of personal and sensitive data.

The organisation recognises that these categories are interrelated and that a single issue may present risks across multiple areas.

---

6. Risk Management Principles

Neuro Gateway Support Network adopts a number of core principles in its approach to risk management.

Risk management must be proactive, with potential risks identified and addressed before they escalate into incidents. It must be systematic and consistent, ensuring that risks are assessed and managed using a structured approach.

The organisation is committed to proportionality, ensuring that responses to risk are appropriate to the level of threat. Transparency and accountability are essential, and all significant risks must be recorded and reviewed.

The organisation also recognises the importance of learning from experience. Incidents and near misses will be reviewed to identify lessons and improve future practice.

---

7. Roles and Responsibilities

The trustees of *Neuro Gateway Support Network* hold overall responsibility for risk management. They are responsible for ensuring that appropriate systems and processes are in place, that risks are identified and monitored, and that risk management is integrated into governance and decision making.

A designated individual may be appointed to oversee the organisation's risk management processes, including maintaining the Risk Register and supporting the identification and assessment of risks.

All individuals acting on behalf of the organisation have a responsibility to remain alert to potential risks in their work, to follow established procedures, and to report concerns promptly. Risk management is a shared responsibility and must be embedded in everyday practice.

---

8. Risk Identification

Risk identification is the first stage of effective risk management. Risks may be identified through a range of sources, including day-to-day service delivery, client interactions, feedback, internal discussions, incident reports, and changes in the external environment.

Individuals are expected to consider potential risks in all aspects of their work, including risks to individuals, risks arising from organisational processes, and risks associated with external factors such as changes in legislation or service provision.

Once identified, risks must be clearly recorded, including a description of the risk, the circumstances in which it may arise, and any immediate concerns.

---

9. Risk Assessment

Following identification, risks must be assessed to determine their significance. This involves evaluating both the likelihood of the risk occurring and the potential impact if it does. Likelihood may range from rare to highly probable, while impact may range from minor inconvenience to significant harm, including serious injury, legal consequences, or reputational damage.

The organisation uses this combined assessment to categorise risks as low, medium, high, or critical. This categorisation informs the level of response required and the urgency with which the risk must be addressed.

Risk assessments must be documented clearly and reviewed regularly, particularly where circumstances change.

---

10. Risk Control and Mitigation

Once a risk has been assessed, appropriate measures must be implemented to reduce or manage it. This may include introducing or strengthening procedures, providing training, clarifying roles and responsibilities, or implementing additional safeguards.

Preventative measures aim to reduce the likelihood of a risk occurring, while contingency measures aim to reduce the impact if the risk does occur.

The organisation recognises that not all risks can be eliminated. In such cases, risks must be managed to an acceptable level, and the rationale for this must be clearly documented.

---

11. Risk Register

Neuro Gateway Support Network will maintain a Risk Register as a central record of identified risks. The Risk Register will include a detailed description of each risk, its assessed likelihood and impact, the level of risk, actions taken to mitigate the risk, and the individual responsible for oversight.

The Risk Register will be reviewed regularly by trustees and updated as necessary to reflect changes in circumstances. It is a key governance tool and will inform strategic planning and decision-making.

---

12. Incident Reporting and Management

An incident is defined as any event or occurrence that results in, or has the potential to result in, harm, loss, or disruption. This may include safeguarding concerns, data breaches, complaints, or operational failures.

All incidents must be reported promptly and recorded accurately. The organisation will assess the nature and severity of each incident and take appropriate action to address it.

Where required, incidents will be reported to relevant external authorities, such as safeguarding teams or the Information Commissioner's Office. The organisation is committed to learning from incidents and will review them to identify improvements in practice.

---

13. Safeguarding and High-Risk Situations

Safeguarding risks are treated as a priority within the organisation's risk management framework. Any indication that an individual may be at risk of harm must be addressed immediately in accordance with the Safeguarding Policy.

High risk situations, including those involving immediate danger or crisis, require urgent action and may involve referral to emergency services or statutory authorities.

Safeguarding considerations take precedence over other risk management processes where there is a risk to safety or wellbeing.

---

14. Data Protection and Information Risk

The organisation recognises that the handling of personal data presents specific risks, including unauthorised access, loss, or misuse of information.

All data must be handled in accordance with the organisation's Data Protection Policy. Appropriate security measures must be in place, and any breaches must be reported and managed promptly.

15. Monitoring and Review

Risk management is an ongoing process and must be reviewed regularly. The organisation will monitor risks through review of the Risk Register, analysis of incidents, and feedback from service users and stakeholders.

Trustees will review risk management arrangements periodically to ensure that they remain effective and appropriate. This includes assessing whether existing controls are sufficient and whether new risks have emerged.

16. Training and Awareness

Neuro Gateway Support Network is committed to ensuring that all individuals involved in its work understand the importance of risk management and their role in identifying and managing risks.

Individuals will be expected to familiarise themselves with this policy and to apply its principles in practice. Where necessary, additional guidance or training will be provided.

17. Policy Review

This policy will be reviewed annually, or sooner if required, to ensure that it remains aligned with current legislation, guidance, and best practice, and reflects the organisation's evolving activities.

18. Final Statement

Neuro Gateway Support Network is committed to managing risk in a structured, responsible, and proactive manner. By identifying potential risks, implementing appropriate controls, and learning from experience, the organisation aims to protect those it supports, maintain public confidence, and ensure the safe and sustainable delivery of its services.

Risk management is an integral component of good governance and is essential to achieving the organisation's objectives while upholding its values and responsibilities.