Neurameet

NEURAMEET - DATA PROTECTION IMPACT ASSESSMENT (DPIA) GUIDANCE

What is a DPIA?

A Data Protection Impact Assessment (DPIA) is a systematic process designed to identify and mitigate data protection risks associated with any new project or processing activity. As the data controller, schools are typically responsible for completing this assessment to ensure compliance with data protection regulations.

Neurameet has developed this comprehensive guidance to support our educational partners in fulfilling their DPIA requirements under the UK General Data Protection Regulation (UK GDPR). This document provides detailed insights into how personal data is processed within the Neurameet meeting management platform, alongside practical guidance for conducting your assessment.

This template can serve as either a complete foundation for your DPIA or as supplementary material to enhance your existing assessment framework. Schools may adapt this document to align with their specific circumstances and institutional requirements.

Important Legal Notice: Neurameet cannot provide legal advice, and nothing in this document should be considered as such. This information does not replace the need to review guidance from the Information Commissioner's Office or to seek independent legal counsel where appropriate.

STEP ONE: IDENTIFY THE NEED FOR A DPIA

[Explain broadly what the project aims to achieve and what type of processing it involves. Reference relevant documents and summarise why you identified the need for a DPIA.]

Neurameet

Neurameet is utilised to record, transcribe, analyse and generate insights from educational meetings including governance sessions, safeguarding reviews, staff meetings, and parent consultations. The platform enables schools, trusts and local authorities to maintain accurate records, track actions, and meet their statutory obligations regarding documentation and reporting. When providing the Neurameet platform, Neurameet acts as the Data Processor on behalf of schools, multi-academy trusts and local authorities (the "Data Controller").

Under Article 35 of the UK GDPR, a controller must conduct a Data Protection Impact Assessment where processing is likely to result in a high risk to individuals. While the Data Controller ultimately determines whether a DPIA is required, Neurameet has prepared this DPIA recognising that the Data Controller's use of our platform is likely to involve processing personal data relating to children on a considerable scale, including special category and sensitive personal data such as health information, safeguarding concerns, behavioural issues and academic performance. This DPIA therefore provides comprehensive information on the processing operations associated with the Neurameet platform.

STEP TWO: DESCRIBE THE PROCESSING

Describe the nature of the processing

[How will you collect, use, store and delete data? What is the source? Will you share data? What types of high-risk processing are involved?]

The Data Controller determines how and why personal data is processed; however, Neurameet provides the following overview of how personal data is typically collected and processed in connection with the Data Controller's use of our platform:

1. **Collection:** Meeting data is captured through audio recordings initiated by authorised users during school meetings. Participants are made aware of recording through platform notifications.

2. **Processing operations:** Neurameet understands that each Data Controller will undertake the following processes:

    - Recording meetings and capturing participant contributions
    - Transcribing audio to text using automated speech recognition
    - Generating AI-powered summaries, minutes and action items

Neurameet

- Storing and organising meeting records
- Distributing minutes and tracking action completion
- Deleting data according to retention schedules

3. **Storage:** Neurameet's infrastructure and data storage are hosted within secure cloud platforms in the UK, ensuring data sovereignty.

4. **Third parties:** We integrate with carefully selected third-party services for speech-to-text transcription (Speechmatics UK) and AI processing (OpenAI). All sub-processors operate under strict data processing agreements. A comprehensive list of our authorised sub-processors is maintained and available upon request.

5. **Deletion:** The platform enables Data Controllers to configure their own retention policies. Audio recordings are automatically deleted after 30 days. Transcripts and minutes can be retained for up to 2 years or deleted earlier upon request. All data is permanently destroyed when the Data Controller terminates their contract with Neurameet.

Describe the scope of the processing

[What is the nature of the data? Does it include special category data? Volume and frequency? How many individuals are affected?]

The personal data processed by Neurameet consists of meeting-related data provided by the Data Controller. The categories of personal data may include:

Student/pupil data discussed in meetings:

- Names, year groups, and identifying information
- Academic performance and progress
- Attendance and punctuality records
- Behavioural incidents and interventions
- Special Educational Needs and disabilities (SEND)
- Safeguarding concerns and welfare issues
- Medical conditions and health needs
- Family circumstances and support requirements

Neurameet

Staff data:

- Names, roles and voice recordings of meeting participants
- Professional opinions and observations
- Performance management discussions
- Training and development needs
- Absence and welfare matters

Parent/guardian/carer data:

- Names and contact details discussed in meetings
- Engagement and communication records
- Concerns raised and support provided

*Sensitive Data includes:**

- Racial or ethnic origin
- Religious or philosophical beliefs
- Health data and medical conditions
- Special Educational Needs information
- Safeguarding and child protection records
- Children in care status
- Court orders and legal proceedings
- Free School Meal eligibility

*Much of this sensitive data constitutes 'special category data' under UK GDPR requiring additional protection.

The data will be updated continuously through regular meetings for all current and historical students, parents/guardians and staff members within the educational institution.

Neurameet

STEP THREE: CONSULTATION PROCESS

Consider how to consult with relevant stakeholders

[When and how will you seek individuals' views? Who else needs to be involved? Do you need expert assistance?]

The Data Controller may choose to consult with relevant stakeholders, including staff, governors, and parent representatives.

It is important to note that Neurameet, as a Data Processor, has engaged in ongoing consultation with Data Controllers (schools, multi-academy trusts and local authorities) throughout the development and implementation of our platform to ensure it meets operational and legal requirements effectively. We have also consulted with security experts and data protection specialists in architecting our infrastructure and ensuring our Information Security Management System adheres to industry standards.

STEP FOUR: ASSESS NECESSITY AND PROPORTIONALITY

Describe compliance and proportionality measures

[What is your lawful basis? Does processing achieve your purpose? Are there alternatives? How will you ensure data quality and minimisation?]

Lawful basis: As Neurameet acts as a Data Processor for schools and education authorities (the Data Controller), the Data Controller determines the lawful basis for processing. The relevant lawful basis(es) typically include compliance with legal obligations (maintaining meeting records) and legitimate interests (efficient administration and safeguarding).

Does processing achieve the purpose? The Data Controller uses Neurameet for effective meeting management and to meet statutory documentation requirements. The automated recording and transcription is considered necessary to enable schools to fulfil these operational

and statutory requirements accurately and efficiently. It's important to note that similar processing activities may already occur within schools through manual minute-taking, so adopting Neurameet enhances rather than fundamentally changes existing processes.

Are there alternatives? The Data Controller determines whether alternatives exist. However, Neurameet understands that maintaining accurate meeting records is essential for schools to discharge their governance, safeguarding and administrative obligations effectively.

Preventing function creep: As Neurameet acts as a Data Processor, we can only process personal data on the instructions of the Data Controller. This means all processing is approved by the Data Controller and Neurameet cannot process personal data for its own purposes.

Data quality and minimisation: Meeting participants control what information is discussed and recorded. The platform includes features for editing transcripts to ensure accuracy and removing irrelevant content. Data Controllers can configure retention policies to ensure data is not kept longer than necessary.

Information to individuals: Participants can access their meeting records through the platform. As the Data Controller, schools are responsible for communicating with individuals about data processing.

Supporting rights: Neurameet has implemented robust security measures to minimise breach risks and includes built-in tools to assist with subject access requests, deletion requests, and retention policy management.

Sub-processor compliance: We conduct regular due diligence on our sub-processors to ensure they maintain appropriate security certifications and adhere to GDPR obligations.

International transfers: Our primary infrastructure is UK-based. Where international transfers occur (e.g., to OpenAI for AI processing), we ensure appropriate safeguards are in place including Standard Contractual Clauses with UK Addendum or reliance on adequacy decisions.

Neurameet

STEP FIVE: IDENTIFY AND ASSESS RISKS

Neurameet has conducted an assessment of potential risks associated with the processing to assist Data Controllers in meeting their obligations under Article 35. As Neurameet is a Data Processor, this analysis is provided for guidance, and Data Controllers should conduct their own risk assessment.

Risk Description & Impact	Likelihood	Severity	Overall Risk
Unauthorised Access to Meeting Platform • Risk to individuals: Potential disclosure of sensitive personal data • Compliance risk: Breach of UK GDPR; breach of DfE security policies • Organisational risk: Reputational damage, ICO sanctions	Possible	Material	**Medium**
Infrastructure Breach • Risk to individuals: Mass disclosure of meeting records • Compliance risk: Significant UK GDPR breach • Organisational risk: Severe reputational damage, substantial ICO fines	Remote	Severe	**Medium**

Neurameet

Risk Description & Impact	Likelihood	Severity	Overall Risk
Excessive Data Retention • Risk to individuals: Personal data retained beyond necessity • Compliance risk: Breach of data minimisation principle • Organisational risk: Increased exposure to breach impact	Possible	Minimal	**Low**
Inadequate International Transfer Safeguards • Risk to individuals: Reduced data protection in third countries • Compliance risk: Breach of international transfer requirements • Organisational risk: Regulatory enforcement action	Possible	Material	**Medium**
Safeguarding Data Exposure • Risk to individuals: Potential harm to vulnerable children • Compliance risk: Serious breach of safeguarding duties • Organisational risk: Criminal liability, loss of operating license	Remote	Severe	**High**

Neurameet

Risk Description & Impact	Likelihood	Severity	Overall Risk
AI Hallucination in Meeting Minutes • Risk to individuals: Incorrect decisions affecting pupils/staff • Compliance risk: Inaccurate official records • Organisational risk: Governance failures, legal challenges	Possible	Material	**Medium**

STEP SIX: IDENTIFY MEASURES TO REDUCE RISK

The table below identifies the comprehensive measures Neurameet has implemented to address the risks identified in Step Five.

Risk	Mitigation Measures	Effect on Risk	Residual Risk
Unauthorised Platform Access	• Strong password policy with regular rotation requirements • Multi-factor authentication (MFA) mandatory for all users • End-to-end encryption for all data transmissions • Automatic session timeout after inactivity	Reduced	**Low**

Neurameet

Risk	Mitigation Measures	Effect on Risk	Residual Risk
	• Granular role-based access control (RBAC)		
Infrastructure Breach	• UK-based data centres with physical security controls • Network segmentation and firewalling • 24/7 security monitoring and incident response • Infrastructure hardening following NCSC guidelines • Regular security patches and updates	Reduced	**Low**
Excessive Data Retention	• Regular retention policy audits • User-initiated deletion capabilities • Clear retention schedule documentation	Reduced	**Low**
International Transfer Risks	• Primary infrastructure in UK data centres • Standard Contractual Clauses with UK Addendum for US transfers	Reduced	**Low**

Neurameet

Risk	Mitigation Measures	Effect on Risk	Residual Risk
	• Annual sub-processor compliance audits • Contractual data protection obligations for all processors • Transfer impact assessments maintained		
Safeguarding Data Exposure	• Strict access controls for sensitive meetings • Ability to restrict meeting access to specific roles • Complete audit trail of all data access	Reduced	**Low**
AI Accuracy Issues	• Clear labelling of AI-generated content • Human review requirement before finalisation • Edit capabilities for all generated content • Version control and change tracking • Regular AI model accuracy assessments • User training on AI limitations	Reduced	**Low**

Neurameet

Evaluation: With the comprehensive mitigations implemented above, the residual risk levels are assessed as Low and acceptable in relation to the substantial benefits provided by the Neurameet platform for efficient and accurate meeting management in educational settings.

STEP SEVEN: SIGN OFF AND RECORD OUTCOMES

[To be completed by the Data Controller]

Item	Name/Date	Notes
Measures approved by:	_____	Integrate actions into implementation plan with dates and responsibilities
Residual risks approved by:	_____	If accepting any residual high risk, consult the ICO before proceeding
Consultation responses reviewed by:	_____	If decision departs from stakeholder views, document reasoning
DPO advice provided:	_____	Where applicable, include Data Protection Officer recommendations
Summary of DPO advice:	[Space for DPO advice]	
DPIA will be reviewed by:	_____	Specify review frequency (e.g., annually)
DPIA completion date:	_____	Date this assessment was completed
Next review date:	_____	Schedule review within 12 months

Neurameet

HOW TO COMPLETE THIS DPIA

For Schools (Data Controllers):

1. Review all sections for accuracy in your context
2. Complete fields marked with brackets [...]
3. Assess risks based on your specific environment
4. Document any additional mitigations you implement
5. Obtain necessary approvals and sign-offs
6. Schedule regular reviews

Key Considerations:

- Consult your Data Protection Officer if available
- Consider stakeholder views (staff, governors)
- Document any high residual risks
- Update when processing changes significantly
- Keep as a living document
- Store securely with restricted access

ADDITIONAL RESOURCES

- **ICO DPIA Guidance:** ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

Neurameet

- **DfE Data Protection Toolkit for Schools:** Available from GOV.UK
- **Neurameet Support:** security@neurameet.com

VERSION CONTROL

- **DPIA Template Version:** 1.3
- **Last Updated:** May 2025
- **Next Review:** May 2026

This DPIA guidance is provided for informational purposes only and does not constitute legal advice. Schools should seek independent legal counsel to ensure compliance with their specific regulatory obligations.