



**National
Neurodiversity
Assessments**

| EXPERT ASSESSMENT • PERSONALISED SUPPORT |

Privacy Policy

Date of policy:	September 2024
Last policy review date:	September 2026
Next Policy review date:	September 2027
Person/s responsible:	Registered Manager

This policy is under regular review. Updates will be made to reflect developments in procedures and best practice

Introduction

National Neurodiversity Assessments (trading under Speech and Language Therapy West Midlands Ltd) provides autism and ADHD assessments and related clinical services.

We are committed to protecting personal information and handling it lawfully, transparently, and securely in accordance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- CQC Fundamental Standards
- Relevant professional regulatory standards

We recognise that much of the information we process is special category health data, and we apply enhanced safeguards accordingly.

Rodney Clinical Portal Transparency Information

This privacy policy applies to the Rodney Clinical Portal and associated NHS Right to Choose autism and ADHD assessment services operated by Speech and Language Therapy West Midlands Ltd / National Neurodiversity Assessments.

Rodney is a secure cloud-hosted clinical portal used by authorised administrators, clinicians and management staff to manage referrals, waiting lists, screening questionnaires, clinical documentation, safeguarding workflows, reporting and operational governance activities.

There is currently no direct patient access to Rodney.

AI-assisted clinical documentation – Heidi Health

We use Heidi Health as an AI-assisted clinical documentation tool during some autism and ADHD assessment and clinical consultations.

Where Heidi is used, the clinical conversation may be transcribed in real time and processed to generate draft clinical documentation. Clinicians may also provide relevant contextual information or dictation.

Heidi is used to support clinical documentation. It does not make autism or ADHD diagnostic decisions or other clinical decisions on behalf of our clinicians. All AI-generated transcripts, summaries and draft documentation are reviewed by the responsible clinician before they are relied upon or entered into the clinical record.

Controller and Processor Arrangements

Speech and Language Therapy West Midlands Ltd acts as the Data Controller for personal data processed within Rodney.

Technical providers including Google Firebase / Google Cloud Platform and Google Workspace act as processors or subprocessors under written contractual arrangements including data protection terms and security obligations.

NHS commissioners, GP practices or NHS Trusts may act as independent or joint controllers where information is shared as part of NHS Right to Choose pathways or wider direct care responsibilities.

Heidi Health Ltd acts as a processor when we use the Heidi Health platform for AI-assisted clinical documentation. Heidi processes personal information on our documented instructions under a Data Processing Agreement. Heidi may use approved subprocessors to provide elements of the service, subject to contractual data protection and security requirements.

Governance and Oversight

Information governance, privacy and security controls relating to Rodney are reviewed regularly through organisational governance processes including:

- Clinical Safety Governance Group (CSGG)
- SIRO oversight
- Information governance review
- Data protection impact assessment review
- Business continuity planning
- Cyber security monitoring
- Access review and audit processes

Our Contact Details

Speech and Language Therapy West Midlands Ltd is the Data Controller for the purposes of UK data protection legislation.

Data Protection Officer: Dr Sarah Titchen

Phone Number: 07828995438

E-mail: mdt@nationalneurodiversityassessments.co.uk

Lawful Basis for Processing

We process personal information using the lawful bases that apply to the particular service and processing activity.

For NHS-commissioned health and care services, our primary lawful basis under UK GDPR Article 6 is **Article 6(1)(e) – public task**, where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.

For other services, including privately commissioned or self-funded services, the appropriate lawful basis may differ depending on the nature and circumstances of the processing.

Where we process **special category data**, including health information, we also rely on an applicable condition under **Article 9 UK GDPR**, including where appropriate:

- Article 9(2)(h) – provision of health or social care or treatment and management of health or social care systems; and
- other applicable Article 9 conditions where required by the particular processing activity.

We may rely on **consent** where consent is the appropriate lawful basis for a particular processing activity, such as certain optional recordings or other optional uses of information. Where consent is relied upon, it can be withdrawn at any time. We may also process personal information where necessary to comply with legal obligations or for other lawful purposes permitted under UK data protection law.

The Type of Personal Information We Collect

We currently collect and process the following information in accordance with NHS information governance standards:

- Personal identifiers, contacts and characteristics

- Medical and developmental history
- Educational records and reports
- Previous assessments and diagnoses
- Behavioural observations and assessment results
- Family medical history relevant to autism and ADHD assessments
- Reports from other healthcare professionals
- School or workplace observations
- Medication history (if applicable)
- Assessment scores and clinical observations
- Video recordings of assessments (where explicit consent is given)
- Questionnaire responses from parents, teachers, and other professionals
- Clinical notes and transcriptions
- Audio/conversation data processed during consultations where an AI scribe is used
- AI-generated transcripts, summaries and draft clinical documentation

AI-assisted clinical documentation (Heidi Health)

During some consultations, we use Heidi Health, an AI-assisted clinical documentation tool, to help clinicians document the consultation.

Before Heidi is used, the clinician will explain its use to you and how your information will be processed. If you do not agree to the use of Heidi, the clinician will use the usual manual documentation process instead. Choosing not to use Heidi will not affect your access to our assessment or clinical services.

Heidi may process the clinical conversation and relevant clinician inputs to generate a transcript and draft clinical documentation. The clinician reviews and verifies the output before it is used or entered into your clinical record.

Heidi is not used to make your diagnosis or other clinical decisions. The final clinical interpretation and decisions remain the responsibility of your clinician.

Children and Young People's Data

We provide services to children and young people and process their personal data in accordance with applicable legal and professional requirements.

Where appropriate:

- Consent is obtained from individuals with parental responsibility
- The views and rights of the child are considered in line with their age and understanding
- Gillick competence is assessed where relevant

We take additional care to ensure that children's data is handled sensitively and securely.

How We Get Personal Information and Why We Have It

Most of the personal information we process is provided to us directly by the individual or authorised third party for one of the following lawful purposes:

- When a referral is submitted for assessment/therapy
- When we request details about our services
- When an individual enquires about joining Speech and Language Therapy West Midlands Ltd
- When an individual works with a member of our team, such as an assessor
- When an individual completes pre-assessment questionnaires
- When an individual provides developmental history information
- When we are sent previous medical or educational reports
- When we record assessments for clinical documentation purposes

We also receive personal information indirectly, from the following sources in accordance with NHS information sharing protocols:

- Schools and educational institutions providing academic records
- Healthcare professionals sharing relevant medical history
- Local authorities providing information about previous interventions
- Other clinicians involved in the person's care
- Professional referrers providing background information
- NHS and other healthcare providers as part of integrated care pathways

How We Use Your Personal Information

We use the information that you have given us to:

- Carry out Speech and Language Therapy services in accordance with NHS service specifications

- Conduct autism and ADHD assessments following NICE guidelines
- Provide reports and recommendations to relevant professionals
- Coordinate with other professionals and services
- Plan appropriate support and interventions
- Meet our legal obligations and NHS contractual requirements
- Maintain clinical records for continuity of care
- Support quality improvement and clinical audit activities
- Comply with safeguarding responsibilities

Data Accuracy

We take reasonable steps to ensure that personal data is accurate, complete, and kept up to date.

Individuals are encouraged to inform us of any changes to their personal information.

Where inaccuracies are identified:

- Corrections are made promptly
- Records are updated with an audit trail where appropriate

Clinical records and reports are reviewed prior to finalisation to ensure accuracy and appropriateness.

Confidentiality and Data Minimalization

We collect only the minimum necessary information required to provide safe and effective care.

Data Minimisation

We only collect and process personal data that is necessary for the provision of safe and effective clinical care and to meet legal and contractual obligations.

We do not collect excessive or irrelevant information.

Where possible, data is anonymised or pseudonymised for audit, service improvement, and reporting purposes.

All staff are bound by confidentiality obligations as part of their employment or contractual terms.

Technology Systems and Data Processing

Patient Management Portal - Google Firebase

We use Google's Firebase suite for our patient management portal:

- **Data Processing Agreement:** Comprehensive Data Processing Addendum (DPA) automatically forms part of Google Cloud Terms of Service
- **Legal Framework:** Legally-binding document outlining Google's data protection responsibilities
- **Compliance:** Subject access request handling and data protection law compliance
- **Security:** Enterprise-grade security with encryption and access controls
- **Data Location:** UK/EU data processing and storage
- **NHS Standards:** Compliant with NHS Data Security and Protection Toolkit requirements

AI-assisted clinical documentation – Heidi Health

We use Heidi Health as a processor for AI-assisted clinical documentation during approved clinical consultations.

Heidi processes clinical conversation data and relevant clinician inputs to provide transcription and generate draft clinical documentation.

Access to Heidi is restricted to authorised clinicians using approved accounts and devices. Clinicians are required to follow NNA's security, confidentiality and retention procedures.

We maintain supplier due-diligence and contractual arrangements with Heidi Health, including data protection and security requirements.

International Data Transfers

The organisation does not routinely transfer personal data outside the United Kingdom (UK) or European Economic Area (EEA).

Where third-party providers (such as cloud service providers) are used, data is configured to be stored and processed within UK or EEA regions wherever possible.

If personal data is transferred outside the UK or EEA, this will only occur where appropriate safeguards are in place in accordance with UK GDPR, including:

- UK adequacy regulations
- International Data Transfer Agreements (IDTA)
- Standard Contractual Clauses (SCCs) with appropriate risk assessments

Any such transfers will be subject to a Data Protection Impact Assessment (DPIA) and ongoing monitoring.

Google Workspace for Secure Storage

Speech and Language Therapy West Midlands Ltd uses Google Workspace with Google Drive for secure cloud storage:

NHS Data Security Compliance:

- Compliant with NHS Data Security and Protection Toolkit (DSPT) requirements
- Data is stored within the UK and/or European Economic Area (EEA) in accordance with UK GDPR adequacy requirements
- Adherence to NHS information governance frameworks
- Regular NHS compliance audits and reviews
- NHS-approved data sharing protocols

Security Features:

- Multi-factor authentication mandatory for all users
- Advanced encryption for data in transit and at rest
- Regular security audits and updates
- Automatic backup and version history
- Role-based access controls
- Device management and security policies
- Comprehensive audit trails of all data access

- Secure NHS mail integration capabilities (we have secure email accredited to the DCB1596 secure email standard)

Information Sharing and Disclosure

We may share personal information with organisations and service providers where this is necessary to provide healthcare services, operate our systems, meet legal or contractual obligations, safeguard individuals, or otherwise process information in accordance with applicable data protection law.

Where we use third-party processors, such as Heidi Health, they process personal information on our documented instructions under appropriate contractual arrangements and are required to maintain appropriate security and confidentiality.

There are certain circumstances where we may be required to do so in accordance with NHS contractual obligations and legal requirements:

- Safeguarding concerns requiring immediate action
- Where necessary to protect a child or vulnerable adult from harm
- Legal obligations to law enforcement or government bodies
- Court orders or statutory requirements
- NHS integrated care pathway requirements
- Quality assurance and clinical audit (with appropriate anonymisation)
- Serious incident reporting to relevant authorities
- Professional regulatory body requirements
- Liaison with other agencies with appropriate consent or legal basis

Records Management

We follow the NHS Records Management Code of Practice and NHS standard contract requirements:

- **Adult assessments:** 8 years from last contact
- **Child assessments:** Until 25th birthday or 8 years after last contact (whichever is longer)
- **Video and audio recordings:** Maximum 8 years with explicit consent
- **Questionnaires and reports:** 8 years from completion
- **Financial records:** 7 years as required by law
- **Clinical audit data:** In accordance with NHS audit requirements

Data Retention and Disposal

We retain personal data in accordance with the NHS Records Management Code of Practice and applicable legal requirements.

Retention periods include:

- Adult health records: 8 years after last contact
- Children's records: until the 25th birthday (or 26 if 17 at discharge)
- Video/audio recordings: maximum of 8 years where explicit consent has been obtained
- Financial records: 7 years in line with legal requirements

At the end of the retention period:

- Data is securely deleted from electronic systems
- Any residual data is rendered irretrievable
- Disposal processes are documented and auditable

We do not retain personal data longer than necessary for the purposes for which it was collected.

Use of Heidi and retention

When Heidi is used, the consultation transcript and any AI-generated draft documentation are temporary working information used to support the clinical documentation process.

Our clinicians are required to delete the Heidi session within 24 hours after the required clinical documentation has been securely transferred to the approved clinical record system, in accordance with our internal procedure.

The final verified clinical record is retained separately in accordance with our clinical records retention requirements. Deleting the Heidi session does not delete the patient's clinical record.

Data Protection Rights

Under UK GDPR and Data Protection Act 2018, patients have the following rights:

- **Right of access** to your personal data
- **Right to rectification** of inaccurate data
- **Right to erasure** (right to be forgotten)
- **Right to restriction** of processing
- **Right to object** to processing
- **Right to data portability**
- **Right not to be subject to automated decision-making**

Patients are not required to pay any charge for exercising their rights. We will normally respond to requests within one month, subject to the applicable legal requirements.

Requests should include sufficient information to verify identity. We may request identification before releasing information.

Automated Decision-Making

We do not carry out automated decision-making or profiling that produces legal or similarly significant effects on individuals.

All clinical decisions, including diagnosis and treatment planning, involve qualified professionals and human review.

We use AI-assisted tools, including Heidi Health, to support clinical documentation in some consultations.

Heidi does not make autism or ADHD diagnostic decisions, determine eligibility for treatment, or make clinical decisions on our behalf. AI-generated transcripts, summaries and draft documentation are reviewed by a qualified clinician before they are relied upon or entered into the clinical record.

Clinical interpretation and final diagnostic decisions remain the responsibility of the appropriately qualified clinician.

Direct Marketing

Marketing communications are sent only where consent has been given or where permitted under legitimate interests in accordance with the Privacy and Electronic

Communications Regulations (PECR). You have the right to opt out at any time by emailing info@saltwm.co.uk.

Website and Social Media

- We use cookies to collect standard internet log information and visitor behaviour
- We may collect publicly available information from social media when users interact with our profiles
- All website data collection complies with UK GDPR requirements

Data Security Incidents

In the event of a data security incident:

- We will assess and contain the incident immediately
- Notify relevant authorities within 72 hours where required
- Inform affected individuals without undue delay where appropriate
- Implement remedial actions to prevent recurrence
- Report to NHS England and relevant commissioners as per contractual obligations

Data Security Measures

We implement appropriate technical and organisational measures to protect personal data, including:

- Encryption of data at rest and in transit
- Multi-factor authentication for system access
- Role-based access controls (RBAC)
- Secure, NHS-compliant email systems
- Audit logs and monitoring of system access
- Regular system updates and security patching
- Secure remote working protocols

Access to personal data is restricted to authorised personnel with a legitimate need.

All staff are required to follow strict confidentiality and data security procedures.

Staff and Candidate Privacy Notice

Scope

This privacy notice applies to all current and former employees, workers, contractors, applicants, and candidates of Speech and Language Therapy West Midlands Ltd.

What Personal Data We Collect

We may collect and process the following categories of information:

- Identification and contact details (e.g. passport, driving licence, name, address, email, phone, bank details)
- Application and recruitment information (CVs, cover letters, interview notes, references)
- Employment records (contracts, pay, performance, training, absence, appraisal data)
- Professional registration, qualification, and right-to-work documentation
- Health and occupational health information (where necessary and lawful)
- Equality and diversity data (optional, for monitoring purposes)
- Criminal record information (where relevant for safeguarding roles)

Why We Process Staff and Candidate Data

We process this information to:

- Manage recruitment and selection processes
- Establish and maintain employment or contractor relationships
- Comply with legal, regulatory, and safeguarding obligations (including NHS and CQC requirements)
- Administer payroll, pensions, and benefits
- Ensure health, safety, and wellbeing at work
- Conduct performance management, training, and professional development
- Maintain professional registration and compliance with NHS and data security standards

Lawful Bases for Processing

Our lawful bases include:

- Performance of a contract (employment or contractor agreement)
- Compliance with legal obligations (e.g. right-to-work checks, safeguarding)
- Legitimate interests (e.g. business administration, recruitment)
- Consent (where applicable, such as for optional diversity monitoring)

Information Sharing

We may share staff and candidate information with:

- Payroll and pension providers
- HMRC and other government bodies
- NHS organisations (for compliance and verification)
- Professional regulatory bodies (e.g. HCPC, RCSLT)
- DBS (Disclosure and Barring Service) for safeguarding checks
- CQC
- Occupational health providers
- Training and accreditation providers

Data Retention

- Candidate data: retained for up to 12 months after recruitment outcomes (unless consent is given to retain for longer)
- Employment records: retained for 6 years after employment ends
- Payroll/tax records: retained for 7 years as required by law

Your Rights

Staff and candidates have the same UK GDPR rights as outlined earlier in this policy (access, rectification, erasure, restriction, objection, data portability).

How to Complain

If you have concerns about our use of your personal information:

If you have concerns about how your personal data is handled, you should contact our Data Protection Officer in the first instance.

If you remain dissatisfied, you have the right to lodge a complaint with the Information Commissioner's Office, the UK supervisory authority for data protection issues.

We encourage individuals to contact us first so we can resolve concerns promptly and effectively.

Primary Contact:

Data Protection Officer: Dr Sarah Titchen

Phone Number: 07828995438

E-mail: mdt@nationalneurodiversityassessments.co.uk

Data Protection Authority:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire SK9 5AF

Helpline: 0303 123 1113

Website: <https://www.ico.org.uk/>

NHS Complaints:

You may also raise concerns through NHS complaint procedures via your commissioning organisation or NHS England.