Sinclair-Strong Consultants Ltd - Privacy Notice
Version: 2.0 (Effective from 24th February 2026)

1) Who we are

Sinclair-Strong Consultants Ltd ("SSC", "we", "our") is an independent, multidisciplinary mental health and neurodevelopmental service providing specialist assessments, diagnostics and treatment pathways across the UK. Our work includes NHS-commissioned services, such as autism and ADHD diagnostic pathways, as well as private care for individuals seeking tailored psychological support.

We operate from our main base in Kings Hill, Kent, and deliver services in-person, remotely, and through our secure online systems. Our team consists of clinical and forensic psychologists, psychiatrists, occupational therapists, speech and language therapists, positive behaviour support practitioners, and specialist administrators who help coordinate safe and effective care.

As an organisation, we act as a **Data Controller**. This means we are legally responsible for deciding how and why your personal information is used, ensuring it is handled lawfully, ethically, and securely. We comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as well as additional NHS information governance standards when we provide services on behalf of the NHS.

To support safe care delivery, we work with carefully selected partners, for example, technology providers who help us run our secure clinical systems and Patient Portal, but these organisations act only on our instructions under strict data protection agreements.

Your privacy, dignity and safety are central to how we operate. This Privacy Notice explains how we collect, use, store, share and protect your information, and outlines the rights you have over your data. Our aim is to be transparent, clear, and accountable, so you can be confident in how your information is handled throughout your care with us.

2) Scope – who this applies to

This Privacy Notice is designed for people who use our services and anyone directly involved in supporting their care. Because our work spans NHS-commissioned pathways, private assessments and ongoing therapeutic or clinical support, this notice explains how we use information across all these settings.

This notice applies to:

2.1 People receiving care from us

Whether you are referred through the NHS (for example, via an ICB pathway such as Autism or ADHD), or you access our services privately, this notice covers how we use your information throughout your care journey. This includes individuals accessing:

- Neurodevelopmental pathways such as AURAS (Autism) and FLOCUS (ADHD).
- Mental health assessments and psychological therapies.
- Forensic, behavioural, or specialist clinical services; and
- Follow-up care, medication monitoring, or ongoing communication about your treatment.

2.2 People supporting someone receiving care

Sometimes we need to work with other people involved in your wellbeing. This notice applies to the information we may collect or use about:

- Carers, family members or trusted supporters acting on your behalf.
- People with parental responsibility or those legally authorised to make decisions for another adult.
- Advocates, where you have nominated someone to speak or act for you.

We only collect the minimum information necessary about these individuals, typically contact details and verification of their role, and we always do so respectfully and transparently.

2.3 People who communicate or interact with us regarding a patient's care

This includes professionals who contact us in connection with your assessment or treatment, such as:

- Your GP or other NHS clinicians.
- Local Authority or Social Care teams.
- Emergency or crisis services.
- Support workers, mental health teams or voluntary sector partners.

We may receive or share information with these organisations where this is necessary for safe and effective care, safeguarding, or to meet statutory or regulatory requirements.

2.4 Visitors to our website and Patient Portal

If you use our website or Patient Portal, for example, to:

- access your records,
- exchange secure messages,
- complete online forms, or
- manage appointments,

this Privacy Notice explains how we handle the information generated through these tools, including security measures, cookies and analytics preferences.

3) The information we collect and create

To provide you with safe, effective and personalised care, we need to collect and create different types of information about you. We aim to gather only what is genuinely necessary, and we do so with openness, respect and a clear purpose.

Below is a detailed overview of the types of information we handle and why they matter for your care.

3.1 Basic identity and contact details

We collect information that helps us confirm who you are and communicate with you reliably. This includes:

- your name, date of birth and gender.
- your home address, email address and phone number.
- details of trusted contacts such as next of kin or a nominated carer.
- your NHS number (where applicable), which helps us link your care safely across services.

These details make sure we can identify you correctly, contact you about appointments, and coordinate important aspects of your care.

3.2 Health and care information (special category data)

As a clinical service, we process highly sensitive information that is essential for assessment, diagnosis, treatment and follow-up. This may include:

- your referral details and the reasons for your assessment.
- clinical history, mental health history and relevant physical health information.
- notes from appointments, consultations and multidisciplinary discussions.
- results from diagnostic tools used in pathways such as AURAS (Autism) and FLOCUS (ADHD), including structured interviews, questionnaires, observational records and cognitive assessments.
- risk and safety information, including safeguarding concerns, where relevant.
- care plans, treatment recommendations and progress notes.

For some pathways, for example FLOCUS where ADHD medication is part of your ongoing care, we may also record:

- prescribing information.
- medication reviews.
- side-effect monitoring and safety checks.

This information enables us to provide care that is clinically sound, safe and tailored to your needs.

3.3 Information you share with us through communication channels

When you contact us, we may process information from:

- emails you send to us (including documents you attach).
- incoming calls or voicemail messages.
- online contact forms.
- feedback, compliments or complaints you choose to share.
- secure messages sent through our Patient Portal.

This helps us respond to your queries, support you between appointments, and ensure continuity of care.

3.4 Information created or received through our Patient Portal and digital tools

If you use our Patient Portal, we process:

- your login details and profile settings.
- secure messages between you and our team.
- forms, questionnaires and documents you submit.
- documents and letters we share with you digitally.
- portal audit logs (e.g., when you accessed or updated information), which help ensure system security and traceability.

These digital records support more flexible care and give you a clear, accessible way to manage aspects of your health information online.

3.5 Information from other health and social care professionals

To provide whole-person care, we may receive information from organisations involved in your wellbeing, such as:

- your GP.
- NHS Trusts or Integrated Care Boards (ICBs).
- social care teams or local authorities.
- crisis, emergency or safeguarding services.

This may include referral information, reports, previous assessments, or relevant medical history. We only request or use what is strictly necessary for your assessment or treatment.

3.6 Administrative, operational and financial information

To run our services smoothly, we also process information such as:

- appointment bookings and attendance records.
- your preferences for communication or adjustments you need (e.g., accessibility needs).

- invoices and payments for private services (these do not include your clinical records).

This operational information allows us to provide efficient, person-centred services that meet your needs reliably.

3.7 Technical and security information

When you use our website or Patient Portal, we may collect limited technical data that helps keep our systems secure and functioning properly, such as:

- device and browser information.
- IP addresses and session activity.
- strictly-necessary cookies for security and navigation.

We only use analytics or non-essential cookies if you choose to give consent (see the Cookies section for more detail).

3.8 Why we collect this information

Every category of information we collect is tied to a lawful purpose. We use your data to:

- deliver safe, high-quality clinical care.
- communicate with you effectively.
- meet legal, regulatory and NHS requirements.
- protect your safety and wellbeing.
- improve and monitor our services.

We explain these lawful purposes in more detail in Section 4 ("Why We Use Your Information").

4.) Why We Use Your Information (and the Legal Bases That Allow Us To)

To provide you with compassionate, effective and safe care, we need to use your personal information in a number of ways. This section explains why we process your data and the legal bases under the UK GDPR and DPA 2018 that allow us to do so. We are committed to being transparent, so you always understand the purpose behind each use of your information.

4.1 Our overall approach

We only use your information when we have a clear reason and an appropriate legal basis. Because much of what we do involves healthcare which involves sensitive clinical information, we also rely on specific rules for special category data, which require an additional legal condition. Almost all of our clinical activities rely on the following principles:

- We use the least amount of information needed to deliver a safe, high-quality service.
- We do not use your information for anything unexpected or incompatible with your care.
- We tell you when a purpose is optional, and we ask for your consent when this is the lawful basis.

- We keep you informed when information needs to be shared with others involved in your care, or where the law requires it.

4.2 The key reasons we process your information

Below is a table that details the main purposes for which we use your information with the appropriate lawful basis we apply when processing this data:

Purpose	Typical activities	Article 6 Lawful Basis	Article 9 exemption (if special category)
Direct care (NHS)	Assessment, diagnosis, treatment; information sharing with GP/NHS teams; safety & continuity of care	**6(1)(e)** public task; sometimes **6(1)(c)** legal obligation	**9(2)(h)** health & social care
Direct care (Private)	As above for private/self-funded pathways	**6(1)(b)** contract **6(1)(f) legitimate interests**	**9(2)(h)** health & social care
AURAS (Autism) pathway	Diagnostic assessments (incl. structured tools), multidisciplinary reports; GP updates	**6(1)(e)** public task (NHS referrals) or **6(1)(b)** contract (private)	**9(2)(h)** health & social care
FLOCUS (ADHD) pathway	Diagnostic assessments, prescribing & medication monitoring; GP updates	**6(1)(e)** (NHS) or **6(1)(b)** (private)	**9(2)(h)** health & social care
Patient Portal/EPR	Account management, secure messaging, appointment management, document sharing; audit logs & MFA	**6(1)(b)** contract (service provision) and/or **6(1)(e)** (NHS)	**9(2)(h)** health & social care
Safeguarding	Identifying/acting on risks to a child or adult at risk; information sharing with authorities	**6(1)(e)** public task and **6(1)(d)** vital interests	**9(2)(b)** social protection and/or **9(2)(c)** vital interests / **9(2)(g)** substantial public interest
Clinical audit/quality	Audits, incident review, service monitoring	**6(1)(e)** public task/**6(1)(f)** legitimate interests	**9(2)(h)** health & social care
Regulatory/queries	Responding to CQC/ICO/court orders; handling legal claims	**6(1)(c)** legal obligation/**6(1)(f)** legitimate interests	**9(2)(f)** legal claims/**9(2)(g)** substantial public interest
Finance	Invoicing, payment, refunds (no care data used)	**6(1)(b)** contract/**6(1)(f)** LI	N/A

Research/planning (where in scope)	Only where permitted and applying the **National Data Opt-Out**	**6(1)(e)** public task/**6(1)(a)** consent (as appropriate)	**9(2)(j)** research/**9(2)(h)**; NDOO applied where required
Direct marketing (limited)	Service updates/offers to private clients who opt-in.	**6(1)(a)** consent (individuals)	**9**: n/a (no special category data)
Website cookies/analytics	Non-essential cookies/analytics with consent	**6(1)(a)** consent	n/a

5) Who we share you information with and why

We only share your information when it is necessary, lawful and proportionate. Below is a simple summary of who may receive your data and why.

- **Your GP and NHS teams** – to ensure accurate records, safe prescribing and coordinated care.
- **Other health or social care providers** – when they are directly involved in your assessment, treatment or support.
- **Safeguarding teams, police or emergency services** – if needed to protect you or someone else from serious harm.
- **Regulators and legal bodies (e.g., CQC, ICO, courts)** – only when required by law or official investigation.
- **Trusted service providers (Data Processors)** – such as our Patient Portal/EPR provider Leftshift Ltd, IT support and secure communication services, who operate under strict contracts.

We share only what is necessary, only with those who need it, and always under strong confidentiality and security controls.

6) The Patient Portal & Electronic Patient Record

Our Patient Portal gives you a secure, convenient way to access parts of your care online. It is part of our wider Electronic Patient Record (EPR) system, which helps us deliver safe, coordinated care. The Portal lets you:

- View letters, reports and documents we share with you.
- Send and receive secure messages with our team.
- Complete forms or questionnaires related to your assessment or treatment.
- Manage appointments where this feature is available.

How your information is handled

- The Portal is built and hosted by our trusted technology provider, Leftshift Ltd, who acts strictly under our instruction as a Data Processor.
- We use strong security measures, including encryption, access controls and audit logs, to protect your information.

- Only authorised SSC staff involved in your care can access your record.

Why we use the Portal

The Portal helps us deliver care more efficiently and supports clear communication between you and our team. It also provides a secure alternative to email for sharing sensitive information

7) How we keep your information secure

Protecting your information is central to how we work. We use a combination of strong technical systems, professional standards and strict internal processes to keep your data safe at every stage. Our security measures include:

- **Strict access controls** – only staff who need to see your information for your care can access it.
- Encryption – your data is protected during transfer and while stored within our systems.
- **Secure systems and** devices – we use up-to-date security tools, monitoring and protective technologies.
- **Regular training** – all staff receive ongoing training on confidentiality, information governance and data protection.
- **Audit and monitoring** – we keep detailed logs of access to your records and regularly review them to ensure appropriate use.
- **Data Processor checks** – any external providers supporting our clinical systems must meet strict contractual, confidentiality and security standards.

Our approach to confidentiality

Everyone at SSC - from clinical teams to administrative staff - is bound by professional and legal duties to maintain confidentiality. Your information is never shared outside approved purposes, and we continually review our processes to ensure they remain safe and compliant.

If something goes wrong

If we ever identify a data breach or security concern, we will:

- act immediately to contain and investigate it.
- inform you where there is a risk to your rights or privacy.
- meet all legal obligations, including notifying relevant authorities where required.

Our goal is to prevent issues wherever possible and to respond quickly and transparently if they occur.

8) The National Data Opt-Out

The National Data Opt-Out is a national NHS policy that gives you control over whether your confidential patient information can be used for healthcare planning and research beyond your

individual care. It does *not* affect the care you receive, and it does not stop information being shared when it is needed to look after you directly.

How the opt-out works

Some types of research or planning activities use confidential patient information. When these activities fall within the scope of the NDOO policy, organisations like ours must check whether you have chosen to opt out. If you have, we must exclude your information from these uses.

How to set or change your opt-out choice

You can view or change your opt-out status at any time using official NHS services, including:

- the NHS App, under "Your Health, choose if data from your health records is shared for research and planning"
- the online "Your NHS Data Matters" service at https://www.nhs.uk/your-nhs-data-matters/

Our responsibilities

As a health and adult social care provider delivering NHS-commissioned services, we must:

- check your opt-out status before using your data for in-scope planning or research.
- ensure we exclude your data from these uses if you have opted out.
- comply with the NHS England information standard DCB3058, which sets the requirements for National Data Opt-Out compliance.

What the opt-out does *not* affect

Your opt-out does not apply to:

- information used for your direct care (e.g., sharing with your GP).
- situations where we are required by law to share information.
- anonymised data that cannot identify you.

9) How We Store and Protect Your Information Over Time

We take great care to store your information safely throughout your time with us and for as long as we are required to keep it. Our aim is to ensure your data remains secure, accurate and accessible only to those who need it to support your care.

How your information is stored

- Your records are kept within our secure Electronic Patient Record (EPR) system, which uses strong encryption and access controls.
- Paper records (where used) are stored in secure, restricted-access locations and are added to your electronic record as soon as possible.

- Only authorised members of our clinical or administrative teams can access your information, and only when it is needed for your care or for essential service functions.

How we protect your information over time

- We regularly review our systems and processes to ensure your data stays accurate, up to date and secure.
- Audit logs record who accesses your record, helping us ensure confidentiality is maintained at all times.
- We work only with trusted service providers who meet our standards for information security and legal compliance.

How long we keep your information

- We follow the NHS Records Management Code of Practice, which sets the required retention periods for different types of health records.
- For most adult mental health records, this means keeping your information for 20 years from the date of last contact, or 10 years after death (whichever comes first).
- Some records, such as those for young people or specialist services, have different retention periods, and we apply these consistently.
- When the retention period ends, your information is securely deleted or destroyed.

If you leave our service

Your records remain safely stored for the required timeframe, even after your care ends. They are not accessed unless needed for legal, regulatory or safety reasons.

10) International Transfers of Your Information

We aim to keep all your information within the UK whenever possible. However, in certain limited situations, a small number of our trusted service providers may store or process data outside the UK, for example, if they use secure international cloud infrastructure or specialist technical tools.

Our approach to international transfers

If a transfer outside the UK is necessary, we make sure your information remains just as safe as it would be at home. This means:

- We only use reputable providers who meet strict data protection and security standards.
- We implement approved legal safeguards, such as the UK International Data Transfer Agreement (IDTA) or the UK Addendum to EU Standard Contractual Clauses.
- We complete a Transfer Risk Assessment to ensure your information will remain protected to UK GDPR standards.
- We continuously monitor our suppliers to ensure ongoing compliance.

What this means for you

Even if your information is processed outside the UK, it remains fully protected, and your rights stay exactly the same. We will never transfer your data internationally without ensuring robust safeguards are in place.

11) Cookies and Electronic Communications

We want you to feel confident when using our website and Patient Portal. This section explains, in simple terms, how we use cookies and how we communicate with you electronically.

11.1 How we use cookies

Cookies are small files stored on your device that help websites function properly and improve your experience. We keep our cookie use simple and transparent.

Strictly necessary cookies

These cookies are essential for:

- keeping the website and Portal secure,
- enabling core features such as logging in, staying signed in, and moving between pages.

These cookies do not require consent, and you cannot turn them off because they are needed for the site to work.

Analytics or optional cookies

We only use analytics or performance cookies if you choose to allow them. These help us understand how people use our site so we can make improvements, but they are never essential. You are always in control:

- You can accept, reject, or change your cookie settings at any time.
- We will not use optional cookies unless you have actively given consent.

Changes introduced by law

Under the Data (Use and Access) Act 2025, PECR rules are being updated, including increased penalties for non-compliance and changes to certain cookie consent requirements. We continue to monitor these changes and update our practices to remain compliant.

11.2 Electronic communications (email, SMS, Portal messages)

We communicate with you electronically in ways that are safe, respectful and legally compliant.

Service messages

We may send you essential communication about your care, such as:

- appointment reminders.
- instructions for assessments.
- updates about your treatment or the Portal.

These messages are part of delivering your care and do not require marketing consent.

Marketing or optional updates

We only send marketing messages such as optional service updates or information about new offerings if:

- you have explicitly opted in, and
- you can opt out at any time, easily.

This follows PECR rules for electronic marketing.

Portal communications

Sensitive information is shared through the secure Patient Portal rather than standard email. This keeps your personal data protected.

11.3 How to manage your choices

You can:

- change your cookie preferences at any time via our cookie banner/settings.
- withdraw marketing consent whenever you wish.
- ask us to update how we contact you.

We are happy to help if you have questions about cookies or electronic communication, just contact our team.

12) Your rights

You have several rights over your personal information:

1. Right to be informed - You can ask us how we use your information.

2. Right to access your information - You can ask us for a copy of the information we hold about you.

3. Right to correct things - If something is wrong or incomplete, you can ask us to fix it.

4. Right to have information deleted - In some cases, you can ask us to delete your information.

5. Right to limit how your information is used - You can ask us to pause how we use your information.

6. Right to move your information - You can ask us to send your information to you or another provider.

7. Right to object - You can say no to certain uses, for example, marketing.

8. Right to human review - If a computer ever made a decision about you (we don't currently do this), you can ask for a human to check it.

9. Right to withdraw consent - If you've given consent (like for marketing or optional cookies), you can change your mind at any time.

If you want to use any of your data protection rights, such as seeing your information, correcting it, asking us to delete it, limiting how we use it, objecting to something, or withdrawing consent, you can contact us at:

Email: sar@sinclairstrong.co.uk
Post: Data Rights Request, Sinclair-Strong Consultants Ltd, Building 80, Churchill Square, Gibson Drive, Kings Hill, West Malling, Kent ME19 4YU

What happens next

- We may need to confirm your identity to keep your information safe.
- We will respond within one calendar month.
- If your request is complex or involves multiple rights, we may extend this by up to two additional months, but we will always let you know if this happens.

13) Use of Artificial Intelligence (AI)

We use Artificial Intelligence (AI) in a limited and carefully controlled way to support our clinical administration. This helps us work more efficiently, but it does not replace clinical judgement in any part of your care.

What we use AI for

- We use AI-powered tools to assist with the transcription of clinical notes, for example converting dictated or recorded information into written text.
- These tools act like advanced speech-to-text systems, helping our clinicians create accurate records more quickly.

What we *do not* use AI for

- We do not use AI to make decisions about your care.
- We do not use AI to assess, diagnose, profile or predict anything about you.

- We do not use AI to replace clinical judgement or to automate any part of your treatment planning.

How your information stays safe

- AI tools are used in a secure, privacy-protecting environment, under strict contractual and technical controls.
- Your data is only processed to generate accurate clinical notes and **is not used to train AI models.**
- Only authorised staff can access the final written record, and all content is reviewed and verified by a clinician before being added to your clinical file.

Why we use AI in this limited way

Using AI transcription helps:

- reduce administrative time so clinicians can spend more time focused on your care.
- improve the clarity and completeness of clinical notes.
- ensure faster, more accurate documentation.

Your privacy, safety and clinical autonomy remain at the heart of everything we do. If you have questions about how AI is used in your care, we're always happy to explain.

14) How to Raise a Concern or Make a Data Protection Complaint

We want you to feel confident about how your personal information is handled. If you ever have questions or concerns, you can contact us directly, and under the Data (Use and Access) Act 2025, we have a formal complaints handling process to make this as clear and supportive as possible.

Step 1 - Contact Us Directly

Under DUAA, organisations must offer a structured way for people to raise concerns about how their data is handled, before escalating to the ICO. We encourage you to use our internal process first so we can put things right quickly. You can contact us via:

Email:
dpo@sinclairstrong.co.uk (Data Protection Complaints)
complaints@sinclairstrong.co.uk (General complaints)

Post:
Data Protection Complaint, Sinclair-Strong Consultants Ltd, Building 80, Churchill Square, Gibson Drive, Kings Hill, West Malling, Kent ME19 4YU

What we will do:

- Acknowledge your complaint promptly.
- Review it under our formal DUAA-aligned complaints procedure.
- Provide a clear, timely response explaining the outcome and any actions we are taking.

- Keep you informed throughout the process.
  This aligns with DUAA expectations for fairness, transparency and accessible resolution routes.

Step 2 - If You're Not Satisfied

If you feel your concern has not been addressed fully, or you prefer independent advice, you can contact the Information Commissioner's Office (ICO). You do not need to wait for us to finish our process, but DUAA encourages individuals to contact the organisation first where possible.

Post: Information Commissioner's Office (ICO), Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Website: https://ico.org.uk
Telephone: 0303 123 1113

15) Changes to this notice

We may update this notice to reflect changes in law or our services. We will post updates on our website and, where appropriate, notify you directly