Sinclair-Strong Consultants Ltd Privacy Notice

This privacy notice lets you know what happens to any personal data that you give to Sinclair-Strong Consultants Ltd (hereafter referred to as SSC), or any information that we may collect from you or about you from other organisations.

This privacy notice applies to personal information processed by or on behalf of SSC.

This Notice explains:

- Who we are and how we use your personal information.
- What your rights are under Data Protection laws
- Why we need to use your personal information.
- How we lawfully use your personal information.
- Information on teams working within SSC who may need to use your personal information.
- The use of third-party processors
- Where we store your electronic personal information
- Partner organisations who we may share personal information with
- When we can share personal information without consent
- How long we retain your personal information for
- How to raise an object/complaint
- Contact information for our Data Protection Officer and the Information Commissioner's Office

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA18) became law on 25th May 2018. The GDPR is a single EU-wide regulation on the protection of confidential and sensitive information, and the DPA18 implements the regulations into comprehensive UK legislation. Following the decision for the UK to leave the European Union and following the end of the transition period, since January 1st, 2021, the UK has been subject to an Adequacy Agreement which allows data to continue to be shared with European Union Countries without further safeguarding being necessary. This has allowed the European Commission suitable time to grant the UK with adequacy status, meaning The UK has met the required standards in ensuring data transfers to and from the UK are safe. All references to GDPR are now referred to as **UK GDPR**.

For the purpose of applicable Data Protection legislation, including UK GDPR and the Data Protection Act 2018, the organisation responsible for your personal data, referred to as the Data Controller, is **Sinclair-Strong Consultants Ltd,** who are registered with the Information Commissioner's Office with the registration number **Z3233880.**

This Notice describes how we collect, use, and process your personal data, and how in doing so, we comply with our legal obligations to you. Your privacy is important to us, and we are committed to protecting and safeguarding your data privacy rights.

What information does SSC collect?

We collect basic personal data about you, which includes name, address, telephone number, email address, date of birth, next of kin information, NHS number etc. This enables us to provide the appropriate treatment for you.

We will also collect sensitive confidential information known as **"special category personal data,"** in the form of health information, religious beliefs, (if required in a healthcare setting) ethnicity, sexuality, biometric data (if applicable) etc. and we may also receive this information about you from other health providers or third parties.

How does SSC use your information?

The healthcare professionals who provide you with care maintain records about your health and any treatment or care you have received previously. These records help to provide you with the best possible healthcare and treatment.

SSC is a provider of services and uses electronic systems to deliver the most efficient healthcare services to you. However, there may be times when a clinician records paper records, which are then uploaded into your record for completeness. We use a combination of working practices and technology to ensure that your information is kept confidential and secure.

Records about you may include the following information:

- Details about you, such as your address, your carer or legal representative and emergency contact details
- Any contact the organisation has had with you, such as appointments, virtual clinic visits, and emergency appointments.
- Notes and reports about your health
- Details about your treatment and care
- Results of investigations such as laboratory tests, x-rays etc
- Relevant information from other health professionals, relatives, or those who care for you.
- Contact details (including email address, mobile telephone number and home telephone number)

To ensure you receive the best possible care, your records are used to facilitate the care you receive, including contacting you. Information held about you may be used to help protect the health of the public and to help us manage the services we provide. Some of your information will be used for clinical audit purposes to monitor the quality of the services we provide.

How does SSC lawfully use your information?

We need your personal and confidential information to provide you with healthcare services and under the UK GDPR we will be lawfully using your information in accordance with the following legal bases:

Article 6 (1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Article 6 (1)(c) processing is necessary for compliance with a legal obligation to which the controller is subject.

Article 9 (2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems.

SSC may however choose an alternative legal basis dependent on the specific requirements and purpose of the data sharing, including:

- **Consent** – We would obtain freely given, specific, unambiguous, and explicit consent to process your personal data for certain purposes.
- **Contract** – The processing is necessary for a contract we have or wish to enter into.
- **Legal Obligation** – The processing is necessary for us to comply with the law.
- **Vital Interest** – The processing is necessary to protect someone's life.
- **Public Interest** – The processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

Furthermore, if there is a safeguarding concern, then data may be shared to protect the adult or child whose safety is a concern to the healthcare professionals.

We have set out in the table below the conditions within UK GDPR that we rely on when we use your data:

Purpose	Article 6 condition	Article 9 condition
All Patients		
Cooperate with regulators, e.g. the Care Quality Commission	Article 6(1)(e) – public task Article 6(1)(c) – compliance with a legal obligation	Article 9(2)(g) – substantial public interest
Compliance with legal obligations, e.g. a court order requiring us to release information	Article 6(1)(c) – compliance with a legal obligation	Article 9(2)(f) – establishment, exercise, or defence of legal claims Article 9(2)(g) – substantial public interest
Dealing with disputes, for example if you make a legal claim against us	Article 6(1)(f) – legitimate interests (we have a legitimate interest in being able to deal with disputes and legal claims)	Article 9(2)(f) – establishment, exercise, or defence of legal claims
Dealing with any risk to public health	Article 6(1)(e) - public task Article 6(1)(c) – compliance with a legal obligation	Article 9(2)(h) – healthcare and social care purposes Article 9(2)(i) – public health
NHS Patients		
Providing you with our services	Article 6(1)(e) - public task Article 6(1)(c) – legal obligation	Article 9(2)(h) – healthcare

Purpose	Article 6 condition	Article 9 condition
		and social care purposes
Helping to maintain the quality of and improve our services	Article 6(1)(e) - public task Article 6(1)(c) – legal obligation	Article 9(2)(h) – healthcare and social care purposes
Providing assessment report and other clinical information back to your NHS GP surgery	Article 6(1)(e) - public task Article 6(1)(c) – legal obligation	Article 9(2)(h) – healthcare and social care purposes
Helping other organisations delivering NHS or social care to provide you with services.	Article 6(1)(e) - public task/duty of data controller	Article 9(2)(h) – healthcare and social care purposes
Letting you know more about our services and offers, including those from relevant third parties	Article 6(1)(a) - consent	Article 9(2)(a) – consent
Planning and research purposes	Article 6(1)(a) - consent	Article 9(2)(a) – consent
Private Patients		
Providing you with our services	Article 6(1)(b) – performance of a contract	Article 9(2)(h) – healthcare and social care purposes
Providing assessment report and other clinical information back to your NHS GP surgery	Article 6(1)(e) – duty of data controller Article 6(1)(c) – legal obligation	Article 9(2)(h) – healthcare and social care purposes
Helping to maintain the quality of and improve our services	Article 6(1)(f) – legitimate interests (we have a legitimate interest in maintaining and improving the quality of our services)	Article 9(2)(h) – healthcare and social care purposes
Obtaining payment from you for our services	Article 6(1)(b) – performance of a contract	No special category data used
Letting you know more about our services and offers, including those from relevant third parties	Article 6(1)(a) - consent	Article 9(2)(a) – consent
Planning and research purposes	Article 6(1)(a) - consent	Article 9(2)(a) – consent

This Privacy Notice applies to the personal information of service users and any personal information given to us about carers/family members etc.

Who does SSC share information with?

As stated in this Privacy Notice, we may have to share your information, subject to strict contracts and agreements, with any of the following organisations:

- NHS Trusts/Foundation Trusts
- GP Practices
- Integrated Care Boards (ICBs) who are responsible for commissioning health services within your local area.
- Other private sector providers, under contract and to meet lawful obligations.
- Emergency services, if required to facilitate welfare/safeguarding checks
- Social Care Services
- Local Authorities
- Education Services
- Police & Judicial Services
- Other 'data processors,' which you will be informed of

You will be informed who your data will be shared with and in some cases asked for consent for this to happen when this is required.

There are times when we may be required by law to share your information without your consent, for example:

- Where we have an overarching lawful basis that allows us to share, for example, for your direct health care needs. This includes sharing information with your GP if you have been referred under Right to Choose or through a contract your local NHS provider hold with us. We are required to share information, including a copy of the assessment report, to update your GP on your referral, and this information is transmitted using encrypted email and is stored under strict security controls as part of your GP record.
- For private patients we are still required to share information with your GP if you have been diagnosed with a specific condition that must be recorded in your health record and if you have been prescribed medication as it is imperative that your GP record includes this to safeguard you and ensure an accurate updated list of medications is available to those involved in your direct care. If you have concerns about this, you are advised to speak directly with the clinician involved in your care.
- Where there is a serious risk of harm or abuse to you or other people.
- Safeguarding matters and investigations.
- Where a serious crime, such as assault, is being investigated or where it could be prevented.
- Where a formal court order has been issued.
- Where there is a legal requirement, for example if you have committed a Road Traffic Offence.

SSC is committed to ensuring, when required to share personal information, we will endeavour to share only the minimal amount of information as is necessary for the given purpose.

Safeguarding

SSC is dedicated to ensuring that the principles and duties of safeguarding adults and children are consistent and ethically and morally applied, with the wellbeing of all patients being at the heart of what we do.

Our legal basis for processing information for safeguarding purposes, as stipulated in the UK GDPR is:

Article 6 (1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Article 6(1)(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person.

For the processing of special categories data, the basis is:

Article 9(2)(b) – 'processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.

Categories of personal information when handling safeguarding issues

The personal information collected by SSC staff in the event of a safeguarding situation, will be minimised to include only the personal information that is necessary in order to handle the situation in the most appropriate way. In addition to basic demographic and contact information, SSC will also share details of what the safeguarding concern is, which is likely to include special category information, such as health information, medication details if applicable and any additional information that has raised concern. SSC will either receive or collect information in the event that someone contacts the organisation with safeguarding concerns, or we believe there may be safeguarding concerns requiring us to make enquiries to relevant health and social care providers.

We may share information in the most appropriate way to ensure our duty of care as a healthcare provider is evidenced and to enable any investigations as required with other partner organisations such as local authorities, the police or healthcare professionals, it will be carried out in the most appropriate way.

National Data Opt-Out

The National Data Opt-Out (NDOO) allows individuals to choose in specified circumstances if data from their health records is shared for healthcare research and planning. Although SSC is a private provider, we are required to comply with the National Data Opt-Out by having suitable policies, processes, and procedures in place. The service enables individuals to view or change their National Data Opt-Out choice at any time. This can be done:

- through the NHS App by clicking on "Your Health" and selecting "Choose if data from your health records is shared for research and planning"
- online via the NHS data matters page
- by phone, email or post via the manage your choice page

SSC is compliant with the requirements of the National Data Opt-Out and will ensure anybody who has opted out of having their data used for planning and research purposes will not have their data used for any other purpose than their care requirements with SSC.

How does SSC keep your information safe?

- All information you provide to SSC is stored securely. We will take all reasonable precautions to prevent the loss, misuse or alteration of information received.
- All paper forms and correspondence are kept in locked filing cabinets in secure locations.
- Electronic files are stored on encrypted servers and devices, with up-to-date Antivirus and Firewall software.
- Unauthorised access to data is prevented by using restricted permission controls and multi-factor authentication.
- SSC implements the principle of least privilege – only clinicians who require access to specific client data are granted access.
- All information is limited to SSC's administrators, associates and any other personnel required to maintain SSC's services and security.
- SSC is a data controller and any individual employed by SSC is a data controller agent and is required to abide by this privacy statement.
- SSC Partner organisations may be granted access to SSC data to provide services in relation to SSC's own services. In these instances, the Partner organisation becomes a data processor and, in some instances, also a data controller and will have their own privacy statement that complies with the relevant legislation.
- Formal electronic reports transmitted externally are protected using encryption and/or password protection.
- We use secure online platforms which feature end-to-end encryption for online chat, visual-audio calls, visual-audio appointments, and visual-audio meetings to ensure confidentiality.
- SSC may record audio-visual calls, audio-visual meetings, and audio-visual appointments. This is not done without explicit consent from the third party where required. The data may be used for the purposes of reflection, supervision, teaching, training, and research.
- Whilst we endeavour to keep our systems and communications protected against viruses, malware, and other harmful effects, we cannot bear responsibility for all communications not being virus or malware-free.
- Client notes and other documentation are destroyed twenty years after the end of psychological services provided has ended, based on current legal requirements and professional best practice and in accordance with the Records Management Code of Practice 2021.
- In the instance of a data breach, an investigation will be initiated immediately by our acting Data Protection Officer (DPO), and the data subject notified within 72 hours of SSC becoming aware of the data breach.
- Depending on the severity of the data breach it will be reported to the ICO within 72 hours of SSC becoming aware of such a breach.

Your individual data rights

As an individual, you have the following rights in relation to your personal information:

Right to be informed – as a data controller, we are required to inform individuals when their personal information is collected and about the intended purposes behind the processing of that information. This privacy notice ensures as an organisation we satisfy this right. We will ensure we update this notice on a regular basis to ensure you continue to be appropriately informed of how your personal information will be used.

Right to access your personal information– Everybody has the right to access their personal information, as well as information relating to processing activities, and receive a copy of that information. This right is commonly referred to as a Subject Access Request (SAR).

You can also make requests via the following methods:

By Post to the following address: **SAR, Sinclair-Strong Consultants Ltd. Building 80, Churchill Square, Gibson Drive, Kings Hill, West Malling, Kent, ME19 4YU**, providing details on what information you are requesting.

By sending an email to sar@sinclairstrong.co.uk

Verbally when engaged in a call 01732 792022

There is no fee for a Subject Access Request, and you will receive your information within one calendar month from the date of request. For complex requests, we are entitled to apply for an extension of a further 2 months, but you will be informed of this as soon as possible to manage your expectations. To validate any request for information we will need to obtain proof of identity and in the case of third-party requests, the required authority to act must be provided before we can disclose any personal information.

Please be mindful that when we release information to satisfy a Subject Access Request the information is for the **personal use of the requestor only**. It is not to be shared with anybody else and not to be used inappropriately, for example, posting on social media sites. Individuals can be subject to prosecution for posting information in the public domain as ruled by the High Court.

Right to rectification – The correction of personal data when incorrect, out of date or incomplete will be rectified by SSC without undue or excessive delay. If, however, such requests are linked to legally significant matters, such as confirming legal identity, we may require proof of any alleged inaccuracy before we are able to rectify the information held. Please ensure when consulting with Sinclair-Strong Consultants Ltd., we always have the correct contact details for you and be prepared to have personal information checked and verified at every appointment/telephone call.

Right to erasure – Under Article 17 of the UK GDPR individuals have the right to have personal data erased or deleted. This is also known as the 'right to be forgotten.' The right is not absolute and only applies in certain circumstances, for example when your personal data is no longer necessary for the purpose for which it was originally collected or processed. If you wish to make a request to erase personal data, please email (insert email address)

Your erasure request can be instantly fulfilled in respect of live systems, but the data will remain within the backup environment for a certain period of time until it is overwritten.

Right to restrict processing – Article 18 of the UK GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that you can limit the way that the organisation uses your data. This is an alternative to requesting the erasure of your data.

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. If you wish to make a request to restrict the processing of personal data, please email (insert email address)

Right to data portability – Under UK GDPR, individuals have the right to data portability in situations where the personal data that they have provided to SSC is processed by automated means on the basis of consent, or where the personal information is necessary for the performance of a contract. Individuals are entitled to have their personal information transmitted directly from one data controller to another if it is technically feasible to do so. This means being in a structured, commonly used, and machine-readable format.

Right to object to processing – individuals have the right to object to the processing of their personal information on grounds relating to their particular situation and to data processed for direct marketing purposes, however, if we can demonstrate compelling legitimate grounds to process the information then processing can continue. If we did not process any personal information about you and your healthcare

needs, it would be difficult for us to care for and treat you. If you wish to object to the processing of personal data, please email (insert email address)

Rights in relation to automated decision-making and profiling – Automated individual decision-making is a decision made by automated means (i.e., a computer system) without any human intervention. If any of the processes we use rely on automated decision-making, you do have the right to ask for a human to review any computer-generated decision at any point. SSC does not use any automated decision tools or profiling techniques currently if this is to change in the future to enable us to evolve digitally, we will ensure we inform our clients appropriately and keep this notice updated.

How long do SSC store your information for?

When storing your personal information, Sinclair-Strong Consultants Ltd. ensures, as required under UK Data Protection legislation, that we keep your information for the required timeframes and given the nature of the services we provide, we adhere to the NHS Records Management Code of Practice for Health and Social Care and national archives requirements. Adult Mental Health Records are required to be retained for a period of 20 years or 10 years after death with child records retained until the 25th birthday (or 26th birthday if a young person was 17 years of age when treatment ended).
More information on the relevant retention periods can be found in the NHS Records Management Code of Practice 2021

Data Security and Protection Toolkit

As with all health and social care organisations, SSC Ltd is required to submit to the Data Security and Protection Toolkit (DSPT), an online assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 Data Security Standards.
All organisations that have access to NHS patient information and systems must use the DSPT to ensure that they are practising good data security, and that personal information is managed correctly. SSC Ltd submitted to version 7 of the DSPT, for the 2024/25 year in January 2025 and achieved a **Standards Met Status.**

Key Contacts/Complaints

Should you have any concerns about how your personal information is managed, please contact Sinclair-Strong Consultants Ltd. Data Privacy Team in the first instance:

SSC Ltd have a designated Data Protection Officer who can be contacted by:
emailing dpo@sinclairstrong.co.uk

By Post: **DPO, Suite 22, Building 80 Churchill Square, Gibson Drive, Kings Hill, West Malling, Kent ME19 4YU**

By Email: dpo@sinclairstrong.co.uk

If you have a complaint about other aspects of your care, please contact the Team using the below details:

By Post: **Complaints, Suite 22, Building 80 Churchill Square, Gibson Drive, Kings Hill, West Malling, Kent ME19 4YU**

By Email: complaints@sinclairstrong.co.uk

You also have the right to lodge a complaint with the UK's independent authority on data protection issues, the Information Commissioner's Office using the contact details below, and quoting the ICO registration number of: **Z3233880.**

Post: **Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF**
Tel: 01625 545745

Website contact: https://ico.org.uk/