Sinclair-Strong Consultants Ltd

Privacy Statement

Your privacy is of foremost importance to Sinclair-Strong Consultants Ltd. (SSC)

We are committed to responsible and secure use of your data in compliance with the terms of the General Data Protection Regulation (GDPR) 2018. SSC is registered with the Information Commissioners Office (ICO).

SSC has a legitimate interest in processing Personal and Sensitive (Special Category) data to provide psychological and other health related services.

The purpose of this statement is to advise you of what personal information SSC collects and holds, why this data is collected, how long it is kept, and what your rights are regarding the storage of your personal data.

We collect personal information from you through your contact with us.

SSC is a data controller and responsible for its own data management and will abide by this privacy statement.

What information does SSC collect?

SSC collects personal data such as name, address, date of birth, gender, telephone numbers, email address, referrer's details, emergency contact details, GP/medical practitioner details, and employer's details. We also collect any data you, a family member and/or friend provides regarding your personal and family background and potentially sensitive data relating to medical and mental health conditions.

For what does SSC use your information?

We use your information in the following ways:

- To provide clients with mental health, disability, and related services.
- To notify you about changes to your appointments and the services SSC provides.
- To fulfil any administrative, legal, ethical, and contractual obligations.
- On occasions, SSC will provide information on training, workshops, blogs, electronic mailings, or newsletters specific to SSC services only.

What information does SSC share?

We will not share any information about you with other organisations or people, except in the following situations:

- Consent – We may share information with relevant medical professionals, or others whom you have requested or agreed we need to contact.
- Serious harm – We may share your information with the relevant authorities if we have reason to believe that this may prevent serious harm to you or another person.
- Compliance with law – We may share information when the law requires us to, i.e., safeguarding, terrorism, drug trafficking and serious crime.
- Clinical Will – We have a clinical will which means in the event of sudden death or a serious accident or illness, a named colleague will be able to access contact details so we can notify clients.
- Supervision – It is an ethical requirement for any clinician offering mental health, disability, and related services to have regular supervision. Any supervisor used is an accredited member of the relevant accrediting body and works within their ethical framework.

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 that 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.
- 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/or hold their own privacy statement that complies with the GDPR (2018) terms.

- Formal electronic reports transmitted externally are protected using encryption and/or password protection.
- We use Microsoft Teams, which features end-to-end encryption for online chat, visual-audio calls, visual-audio appointments and visual-audio meetings. We may also use alternative encrypted-connection visual audio platforms such as Skype for Business, Zoom, or GoToMeetings, to ensure confidentiality.
- SSC may record audio-visual calls, audio-visual meetings, and audio-visual appointments. This is not done without the 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 the psychological services provided have ended, based on current legal requirements and professional best practice and in accordance with 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.
- Dependant 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.
- Request for personal data we hold for a data subject can be presented via a completed Subject Access Request (SAR) form. We will process your request within one month, however it may take longer if your request is complex. The SAR form is available upon request via:

    - Email: enquiries@sinclairstrong.co.uk
    - Postal addressed to: SAR, Sinclair-Strong Consultants Ltd. Building 80, Churchill Square, Gibson Drive, Kings Hill, West Malling, Kent, ME19 4YU

- SSC's website, www.sinclairstrong.co.uk does not store your data, other than required cookies, should you allow. The website contact request form transmits your details to us without saving any of the data content submitted.
- Client contact details and digital communications with SSC may be stored on computers and mobile devices. All devices containing client data are required to have access restrictions in place and data encrypted for security purposes.

Your rights

Under the GDPR (2018), you have the right to:

1. The right to be informed.
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

- You can withdraw your consent for SSC to store and process your data at any time. However, health care legislation may prevent all or part of your request. You will be advised if this is the case.
- If you withdraw your consent for SSC to store and process your data whilst receiving health, disability and related services provided by SSC, all the services will be discontinued immediately.
- SSC may not be able to delete your data if it relates to health and medical care we have provided to you due to health care legislation. You will be advised if this is the case.
- You can withdraw your consent by stating this in writing or email to: enquiries@sinclairstrong.co.uk
- If you have any concerns about the way SSC stores and processes your data, please contact enquiries@sinclairstrong.co.uk
- If, after contacting us you feel your issue has not been resolved effectively, you have the right to contact the Information Commissioners Office (www.ico.org.uk)

Changes to this policy

This document is regularly reviewed in line with GDPR (2018) Legislation.