SINCLAIR-STRONG CONSULTANTS LTD
CARING FOR MENTAL HEALTH

# Privacy Statement

Your privacy is of great importance to Sinclair-Strong Consultants Ltd (SSC) and we are committed to complying with the terms of the General Data Protection Regulation (GDPR) regarding the responsible and secure use of your data. SSC is registered with the Information Commissioners Office (ICO).

SSC has a legitimate interest in processing personal data to provide psychological and other health related services. The purpose of this statement is to let you know what personal information SSC collects and holds, why this data is collected, how long it is kept, and what your rights are with regard to the storage of your personal data.

When you are referred for mental health, disability or related services with SSC you will be asked to consent to the processing of your data under the terms of this privacy statement. SSC is responsible for its own data management, will abide by this privacy statement, and holds its own privacy statement that complies with GDPR terms.

**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 give us regarding personal and family background, alongside potentially sensitive data relating to medical and mental health conditions.

**What does SSC use your information for?**
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 being caused 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 the 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 as securely as possible. We will take all reasonable precautions to prevent the loss, misuse or alteration of information given.
- All paper forms and correspondence are kept in locked filing cabinets. Electronic files are protected from unauthorised access using technology access controls. All electronic files are kept on password-protected devices with virus protection software. SSC implements the principle of least privilege - Only clinicians that need access to specific client data have access to the data.
- All information is limited to SSC's administrators, associates and any other personnel needed to maintain SSC's services. Any personnel that have access to these files abide by this privacy statement and/or hold their own privacy statement that complies with the GDPR terms.
- Formal reports which are emailed externally are protected using encryption.
- For live chat or audio-webcam appointments, we use Microsoft Teams, which features end-to-end encryption for added security. If Microsoft Teams is not available, we use other platforms that provide encryption such as Skype for Business, Zoom, or GoToMeetings, to ensure confidentiality.
- Whilst we endeavour to keep our systems and communications protected against viruses and other harmful effects, we cannot bear responsibility for all communications being virus free.
- Client notes and other documentation are destroyed twenty years after the end of the psychosocial services offered based on current legal requirements and professional best practice and in accordance with Record Management Code of Practice for Health and Social Care 2016.
- Any known data breaches will be reported to the ICO within 72 hours.
- Any requests for personal data need to be made through a data subject access request and will be supplied within one month.
- SSC's website, www.sinclairstrong.co.uk is maintained by BOnline. Your details are not stored on their systems for any contact requests made through them.
- Client contact details, text messages, and mobile communication on any mobile platform will not be identified as an SSC client and will only be stored on devices that are password protected.

**Your rights**
Under the GDPR, you have the right to:

- Access your personal data - Rectify, erase, or restrict your data - Object to the processing of your data - Request transfer of data (data portability).
- You may withdraw your consent for SSC to hold and process your data at any time. However, if you do this while actively receiving mental health, disability and related services, the services will need to end. You can withdraw your consent by stating this in an email to linda@sinclairstrong.co.uk
- If you have any concerns about the way SSC handles your data please contact linda@sinclairstrong.co.uk If you feel this 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 Legislation.