Dr Laura Shepherd

CPsychol.

Consultant Clinical Psychologist

Tel: 07841 134211

Email: enquiries@laurashepherd-psychologist.co.uk

Web: [www.laurashepherd-psychologist.co.uk](http://www.laurashepherd-psychologist.co.uk)

Practicing from: Dronfield Health and Therapy Clinic, 24 High St, Dronfield, S18 1PY

**Data Protection Policy**

1. This data protection policy is designed to ensure that the rights to privacy of individuals are protected. I am committed to the principles set out in the General Data Protection Regulation (GDPR) and have reviewed my personal data processing activities so as to carry on my business as a sole trader providing psychological assessment, treatment and reports in compliance with the provisions of the Regulation.

2. **Data protection lead:** this person is responsible for ensuring compliance with policies and procedures on data protection, conducting audits, risk assessments and data protection impact assessments, responding to requests from data subjects and dealing with data breaches. He or she also handles queries and complaints from data subjects about the processing of their data. As the sole trader of the company, the name of the data protection lead is Dr Laura Shepherd.

3. ***Data subject:*** an individual whose personal data is processed.

4. ***Personal data:*** any information from which a living individual can be identified, either directly or indirectly. It is not limited to names and identification numbers, or to photographs or addresses.

The categories of personal data the companyprocesses include both personal data and special category data as follows:

***Assessment/Therapy Cases***

* + Names, addresses, dates of birth and other personal data as provided by the client/patient or their rehabilitation company/insurer/solicitor.
  + Health information as provided by the client/patient or their rehabilitation company/insurer/solicitor.
  + Personal data in invoices and copy receipts, accounting records, tax returns and related information;

## Legal cases

* + Names, addresses, dates of birth and other personal data contained in witness statements and other evidence relevant to the legal issues;
  + Health information contained in medical records, together with information on sex, race and ethnic origin;
  + Personal data in invoices and copy receipts, accounting records, tax returns and related information;

***Supervisees***

* + Names, addresses, email addresses and telephone numbers;
  + Professional body registration details;
  + Personal data in supervision contracts;
  + Personal and sensitive data relating to professional practice;

5. **Special category data:** information revealing an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic and biometric data, health information and data in relation to a person' s sex or sexual orientation.

The special category personal data the companyholds includes:

* + Medical and other health records
  + Information on sex, race and ethnic origin

6. ***Processing:*** covers any activity involving personal data, including holding, storage and destruction. The Information Commissioner says it is difficult to image an activity involving personal data that does not fall within the definition.

7. Iprocess personal data in order to carry out my work as a provider of psychological assessments, therapy and expert witness work and when carrying out other functions necessary to my business.

8. The data processing activities include: compiling and storing assessment and therapy notes and reports, compiling and storing expert reports, sending and receiving emails externally, submitting invoices and filing them with receipts, uploading documents onto the cloud, holding supervisees' details on hard copy/electronic files, archiving and destroying information.

9. ***Sharing of personal data:*** Ishare personal data externally only when necessary to achieve my business purposes. In particular, I share data with the following:

* + Digital typing/transcription services
  + Funders, such as rehabilitation companies and solicitors
  + Cloud storage providers
  + Accountants and other professional advisers
  + HMRC

Special category data is encrypted before it is shared. There is no transfer of data abroad.

10. ***Data controller:*** decides the why and the how of personal data processing. A controller can be a sole trader, a partnership, a private or public limited company or a large multi-national organisation. It decides why it needs to collect personal data and how to process it. As a sole trader, Dr Laura Shepherd is the data controller for the purposes of this policy.

11. ***Data processor:*** processes personal data in accordance with the written instructions of the data controller. Dr Laura Shepherd is the sole data processor.

12. ***Legitimising conditions:*** The processing of personal data is unlawful unless a legitimising condition, or lawful basis, applies. I generally rely on the following legitimising conditions:

* + Legitimate interest as a business

When processing special category data, I generally rely on one of the following additional legitimising conditions:

* + Legal claims
  + Explicit consent
  + Processing as necessary for the purposes of medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

Iavoid relying on the consent basis where possible. In order to be valid, consent must be freely given and as easily withdrawn as it was to give it.

13. ***Data protection principles:*** Where there is a lawful basis for processing personal data, I take proportionate steps to ensure I carry out its personal data processing activities in accordance with the various conditions or principles contained in the GDPR.

14. ***Accountability:*** This principle is designed to ensure that data protection is embedded in an organisation at all levels of decision making and becomes fundamental to its culture. Not only must I comply with the General Data Protection Regulation but I must be able to show I comply. It is for this reason that this policy, and the appended policies have been written. Dr Laura Shepherdensures that these policies are implemented.

15. **Data protection by design:** This is an aspect of the accountability principle. It means that data protection risks are evaluated and eradicated and reduced at the very earliest stage, whenever there is a significant change in processes or procedures which entail a risk to data subjects. Examples: a substantial upgrade to an IT system, outsourcing such as engaging a new cloud provider. Data Protection Impact Assessments are carried out by the data protection lead in these and other circumstances where there is likely to be a high risk to data subjects.

16. ***Data protection by default: minimisation:*** Another important principle is data minimisation. In other words, no more data should be collected, shared and stored than is strictly necessary. The retention period for the personal data I store is seven years (or seven years following your 18th birthday if you are a child), as necessary due to legal and professional requirements.

17. ***Security:*** This is one of the most important principles. I have taken physical, organisational and technical measures to ensure that personal data is secure. Hard copy as well as electronic data is processed in accordance with the company’s security policy.

18. ***Personal data breach:*** The data protection lead is responsible for responding to personal data breaches. I will notify the Information Commissioner as necessary, and also data subjects where the risk to them is high.

19. Breaches which carry any risk to data subjects will be reported to the Information Commissioner's Office (ICO) within 72 hours, together with a summary of the nature of the breach, the steps taken to reduce the risk to data subjects, and measures to prevent the breach from happening again. The company has a data breach policy.

20. ***Rights of data subjects:*** Data subjects have eight rights which include:

* Right to be informed about what the company does with personal data;
* Right of access to personal data by means of a subject access request;
* Right to rectification of inaccurate data, and to add to the information the companyholds about the data subject if it is incomplete;
* Right to erasure, otherwise known as the right to be forgotten;
* Right to restrict the processing of personal data;
* Right to object to the processing the companycarries out based on its legitimate interest.

The companymust respond to requests from data subjects within one month. There is a procedure in place for responding to requests.

21. **Data Protection Risk Register:** All personal data processing activities are recorded in the data protection risk register. Personal data breaches are recorded in the risk register, whether they are reportable or not. The risk register contains a copy of all audits, risk assessments and Data Protection Impact Assessments. The data protection lead holds the risk register.

22. **Enforcement and disciplinary action:** Failure to comply with the General Data Protection Regulation is a criminal offence in many cases and can result in large fines.