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 Breach Policy**

1. When there is a personal data breach, as the Information Commissioners Office (ICO) advises, I will:

*Tell it all. Tell it fast. Tell the truth.*

1. The designated data protection lead (Dr Laura Shepherd) is responsible for handling personal data breaches. In particular, she will evaluate what the breach is and how it occurred, and the associated risk to data subjects and the company.
2. If there is a risk to data subjects, the breach will be reported to the ICO within 72 hours. If the report is late, an explanation will be given as to why.
3. Where the risk to data subjects is high, the breach will be reported to them individually if at all possible. If there is a large number of data subjects at risk, it may not be logistically possible to do so, in which case a press release will be given and notification provided on the company website.
4. Encryption of personal data will likely significantly reduce the risk to data subjects following a breach, and I encrypt all personal data such as identification records and medical and health records.
5. The ICO will want to know how the breach occurred, what steps are being taken to reduce the risk, and how a similar breach is to be avoided in future. The initial report will contain no more than a summary of the position. The data protection lead will seek authority to obtain legal advice before submitting the initial and any subsequent reports.
6. A thorough investigation and corrective action will be necessary so as to reduce the risks to data subjects arising out of any breach, and to make sure that something similar does not happen again in future.
7. Where a breach of the company’s computer systems is suspected, the data protection lead will gain the support of the company’s IT provider in order to identify the nature of any breach of computer systems.
8. The theft of data, whether as a result of shortcomings in the physical security arrangements on the premises, or the hacking and penetration of computer systems, will be reported immediately to the police.
9. The breach, investigation and corrective actions will be documented and filed on the data protection risk register, as will the report made to the ICO.
10. All personal data breaches, however minor, and whether reportable or not, will be recorded in the data protection risk register, held by the data protection lead.