Data Protection Policy

Care To Listen adheres to the principles of data protection outlined by the Data Protection Act 1998, namely that personal data will be:

- Processed fairly and lawfully.
- Processed only for specified, lawful and compatible purposes
- Adequate, relevant and not excessive.
- Accurate and up to date.
- Kept for no longer than necessary.
- Processed in accordance with the rights of data subjects.
- Kept secure.

Secure storage of client data

All client information is hosted on a secure internet based Customer Relationship Management system accessible via secure HTTPS. Client records are only accessible to designated staff with specific permissions. Client information is shared only between designated staff.

Paper based records are kept to a minimum. All paper based records are kept securely in a locked cabinet accessible only to the Service Manager.

Retention of data

The organisation keeps client records for up to seven years after clients are discharged, in line with BACP requirements. Any requests will be processed in line with guidelines under the Act.

Access requests (subject access enquiries)

Clients can apply to see any information that Care to Listen holds about them. Clients may request to see any records held at any time according to their rights under the Act and are informed of this before counselling begins. Requests can be made in writing (email or letter), detailing the information required and copies of proof of identity (passport, driving licence or utility bill). It is recommended that clients send letters by Care to Listen will arrange for copies of records to be made available within 40 calendar days of receiving the request.

Anonymisation and Use of Secondary Data

Care to Listen is committed to continuous improvement. In order to monitor the efficacy of the service the organization may use client data to review the service and make improvements. This data will be anonymised and individual clients will not be identifiable from this data.

Data security breaches

All staff are responsible for ensuring that client data is kept secure at all times. All actual and suspected breaches of data security should be reported to the Service Directors.

Training

All staff are provided with information security training at induction and receive regular updates and refresher training on information security.