NWNT

A BESPOKE NEUROPSYCHOLOGY SERVICE

INFORMATION SECURITY POLICY

Paper Records
No paper records are stored permanently. All paper records received if relevant and required are scanned and not stored on the scanning device. They are then uploaded to QuNote or Gsuite whose security standards meet GDPR regulations. The paper version is disposed of confidentially.

Any temporary written notes (e.g. on a telephone call) are identified by initials only and are shredded as soon as possible. Written notes of this nature are kept to a minimum.

Any paperwork stored on a short-term basis with personally identifiable information (PII) will be kept in a locked filing cabinet in a locked room in a secure building.

Electronic Records
Documents including PII that are accessed, stored and processed on electronic devices will be supported by the platforms of QuNote or GSuite. Both of these meet GDPR regulations, including backup. There are no physical external backups kept.

Should you make a request for erasure (see Privacy Policy) you need to be aware that it may be the case that cloud back ups cannot be deleted due to the level of security and encryption under which they operate.

Records are kept in accordance with appropriate record keeping standards (see Service Policy).

Transfer of Documents
Documents that require sharing with other members of a treating or legal team are stored in GSuite and shared through secure systems.

Where possible, PII is not included (for example, no date of birth, initials only, no address) and documents are also encrypted, and password protected. Passwords are shared separately to the document.

If documents are shared by other means, they are encrypted, and password protected. For example, through email.

Where paper documents require transfer, for those including PII recorded delivery postal services are used.

On rare occasions some PII may need to be physically transported, for example taking materials to a training session. Where possible, all PII is removed, using initials only and only brief outlines of clinical or medical details. These are kept from view and any not used are destroyed immediately when completed. However, those who are in receipt of them are bound themselves to follow GDPR standards.

Portable Devices
GSuite and QuNote are used on computers and mobile telephones are also used for accessing, storing and processing PII. All of these platforms are GDPR compliant.

Temporary or downloaded files are removed regularly from computers and computer 'recycle bins / trash cans' are regularly emptied.

The PII will be stored on the platforms themselves and not on the hard-drive of any computer.

Appointment times, telephone numbers and addresses, identified by initials only, may be stored on calendars which require log in details/password to access on either a mobile telephone or computer.

Telephone numbers that are stored under contacts on both telephones and computers are under initials only.

Text, video or photo messages are uploaded to the QuNote system at the earliest opportunity and then deleted or deleted directly if not required to be kept on record.

We have the ability to remotely wipe computers and mobile telephones of all data in the event of loss or theft.

Addresses either non-identified or identified by initials only may be on SatNav history from any visits made to your chosen address.

A Dictaphone may be used for reports and letters. The dictation is identified using initials only. However, there may be other PII in there such as medical history or case details. The dictation is immediately uploaded to the GDPR compliant systems (QuNote, GSuite) and deleted from the device.

Different media may be used to support rehabilitation including written, audio, filming and photographs to be used in a support plan or other in-house documents and not to be shared for any other reason than direct support and care.

General Record Keeping
Anything that is not needed or where information has been taken from it will be deleted electronically or shredded if physical.

Internet & Email
Only secure networks are used to access PII.

Our email platform is Gmail. This meets GDPR standards of encryption. Any PII documents that are emailed rather than transferred through our platforms (see above) are subject to additional password protection, with the password provided separately. Where you have been provided with a password to access documents, it is your responsibility to keep this secure and to not share it.

You can find more information at the ICO website: https://ico.org.uk