NWNT

A BESPOKE NEUROPSYCHOLOGY SERVICE

INFORMATION SECURITY POLICY

This security policy is designed to ensure that NWNT complies with the security requirements of the General Data Protection Regulation, and the rights to privacy of data subjects are protected.

In compliance with Article 32 NWNT has implemented appropriate physical, organisational and technical measures to ensure a level of security appropriate to the risk.

Dr Gemma Wall is based at Lester House, 21 Broad Street, Bury, BL9 0DA. Dr Antonia Kirkby & Dr Gemma Mercer are based at Sutton House, 27 Wilson Patten Street, Warrington, WA1 1PG. There are no employees.

Physical
The office buildings have CCTV and have intercom access external doors. Visitors to the premises are supervised at all times and the office doors are locked unless occupied.

Computer screens are kept from view.

Computers and other electronic equipment are disposed of in a safe manner by an outsourced and certificated provider.

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 using a GDPR compliant shredder. 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.

A clear desk policy is enforced.

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 by myself.

Should you make a request for erasure (see Privacy Policy) you need to be aware that it may be the case that cloud backups 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 your 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
We use GSuite and Qunote on our laptop computers and mobile telephones for accessing, storing and processing PII. All of these platforms are GDPR compliant. Computer and phones are password protected and have automatic locking mechanisms when not in use.

We remove any temporary or downloaded files regularly from our laptops and regularly empty the trash-can.

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

Appointment times, telephone numbers and addresses, identified by initials only, may be stored on calendars which are supported by iCloud/GSuite and requires log in details/password to access on either our mobile telephones or laptops.

Telephone numbers are stored in our contacts on both our telephones and laptops 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 laptops and mobile telephones of all data in the event they are lost or stolen.

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

We use a Dictaphone for reports and letters. We identify the dictation 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.

We may use different media 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 using a GDPR compliant shredder if paper-based.

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 my 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.

Video Conferencing
We have the option of using the following video conferencing platforms for remote working.

- Microsoft Teams
- Zoom
- FaceTime
- Video WhatsApp
- Skype

We work flexibly to use the platform that best suits the client or team and is available to the clinician.

Each platform comes with its own risk and benefits which in summary:

Zoom is encrypted. Although end-to-end encryption is available for additional security this disables many settings and is not standardly used by NWNT. The standard encryption is used.

Skype is encrypted on another Skype number, but not if to another type of number. Can be monitored by Microsoft or Government Agencies.

Microsoft – (see https://support.skype.com/en/faq/fa31/does-skype-use-encryption for more information)

MS Teams is encrypted (https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide)

WhatsApp & FaceTime are end to end encrypted (https://www.whatsapp.com/security/; https://support.apple.com/en-gb/HT209110)

In summary, all video platforms used are encrypted at least the basic level and we use the standard default encryption on these platforms. Please refer to the information from the platforms themselves for further information and use at your own risk.

We will not record the meeting without explicit consent of all parties attending.

We regularly review which platforms we use and would evaluate and report any breaches occurring as a result of these within our policies.

However, we encourage the clients and team to consider which platforms are used and ultimately these platforms are used at your own risk.

Third Parties
We check that systems that we use have their own data protection policies indicating their compliance with GDPR.

Breach Reporting
Breaches and near misses are discussed in Partner's meetings.

We record any breaches that have occurred and the outcomes.

We follow GDPR procedure on Breach reporting, actions and recording. See Service Policy.

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