

Arbor Neurorehabilitation Services Ltd's Website Privacy Policy

Hello there!

Thank you for checking out our privacy policy. At Arbor Neurorehabilitation Services Ltd we take our client's privacy seriously. We're committed to protecting your privacy and handling your information in a responsible way while you use our website and services. Arbor Neurorehabilitation Services Ltd wants you to understand that this is a safe place for you to discuss your feelings and concerns, and Arbor Neurorehabilitation Services Ltd operates in a highly confidential environment. This policy sets out how data is collected and processed through the use of our website and when you access our services.

We encourage you to read this policy alongside any other privacy notices we might provide, so you're fully in the loop about how and why we use your information.

Who's in charge of your data?

The controller of your data is Arbor Neurorehabilitation Services Ltd and we can be contacted on:

Email address: info@arbor-neuro.com

Telephone number: [0117 287 2088](tel:0117 287 2088)

Not happy with something?

Let's chat and try to fix it. You've also got the right to talk to the Information Commissioner's Office (ICO) at (www.ico.gov.org.uk), but we hope to resolve any issues directly.

What type of data do we collect about you?

'Personal data' is information that identifies you. If we've removed your identity (by making the data anonymous), **it won't be classed as personal data**. We might collect, use, store, and share various types of personal data about you as follows:

- **Identity details** such as first and last name, title, date of birth and gender.
- **Contact details** such as your home address, email address and telephone number.
- **Health Data:** information about your or the client's health, including information about existing and previous medical health conditions, diagnoses, developmental and intellectual difficulties, disorders, injury details, neurological injury details, functioning details, medication details, psychiatric history and any other relevant health information to enable us to carry out our services to you. This also includes insurance reports and correspondence with referring professionals e.g., your GP, healthcare practitioners or your case manager.
- **Technical information** such as your internet protocol (IP address), browser type, version, browser plug-in types and versions, time zone setting and location, operating system and platform and other technology on the devices you use to access our website.
- **Financial information** such as your bank account and payment card details.
- **Information about transactions** like details about payments to and from you, and other details of services you have purchased from us.
- **Account details** such as details around the number and frequency of therapy sessions you purchase from us, and your interests, preferences, feedback and survey responses.
- **Usage information** about how you use our website and services.
- **Marketing information** such as your preferences on receiving marketing from both us and third-parties, along with your communication preferences.
- **Associate data** such as the data we hold about members of the Arbor team, which may include personal details, such as date of birth, address, CV and references. We will also store electronic copies of relevant professional documentation, such as DBS checks, evidence of professional indemnity insurance and professional registrations. This data will be stored electronically, with directors of Arbor and administrative staff having access. As an associate you are entitled to request permission to view all data held about you, with references only being disclosed with

permission of the referee. Data will be held for up to 2 years following an associate leaving Arbor such that references can be provided where requested.

Special Category Data – Apart from the Health Data listed above, we do not collect any other Special Category Data about you or your child (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

Consents for Health Data: We require your specific consent to process your Health Data so, when you submit your details, we will ask you to confirm your consent to this processing.

How do we collect your personal data?

We use different methods to collect data from and about you. The majority of the time, our information is collected directly when you contact us in the following ways:

- Correspondence with us via post, phone, email or otherwise;
- When you fill in our 'Make a Referral' form;
- When you complete any forms before or during an appointment;
- Verbally during discussions;
- When you apply for our services;
- When you request marketing communications to be sent to you; or
- When you give us feedback or contact us.

Another method we may use to collect data includes the use of automated technologies or interactions, like website cookies or other similar technologies. This includes information about your equipment, browsing actions and patterns and information about your browsing activity if you visit another website that uses the same cookies as us. This means we receive information about how you use these third-party websites.

This data collection helps us to improve user experience, and to gather information about how you use our website. For more information, please refer to our Cookie Policy, which can be accessed online.

We may also receive data from third-parties such as:

- Parents/Guardians.
- Healthcare professionals, such as case managers;
- Lawyers and expert witnesses;
- Other professionals acting as case managers / referrers; and
- Publicly available sources, such as Companies House and the Electoral Register where legally justified (for example in cases of debt recovery).

What happens if you don't provide us with the required data?

Where we need to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with services such as treatment). In this case, we may have to cancel a service you have with us but we will notify you if this is the case at the time.

What are the purposes for which we use your personal data?

The purposes for which we will be using your data include:

- To register you as a new client.

- To provide our services, including: a) to manage payments, fees and charges and b) to collect and recover money owed to us.
- To manage our relationship with you e.g., to notify you about changes to our terms of this privacy policy or to ask you to leave a review and/or take a survey.
- To send you relevant marketing information about our services.
- To administer and protect our practice and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data).
- To use data analytics to improve our website, services, marketing, client relationships and experiences.
- To make suggestions and recommendations to you about services that may be of interest to you.

We rely on one or more of the following lawful conditions to process your data as outlined above:

- To fulfil our contract with you;
- For our legitimate interests; or
- To comply with legal obligations.

For special category data (e.g., health records), processing is carried out under:

- Article 9(2)(h) UK GDPR – "Provision of health or social care."
- Explicit client consent where applicable.
- Legal obligation when required (e.g., safeguarding concerns).

In some scenarios, we'll ask for your consent, especially for collecting health data. We may process your personal data for more than one lawful reason at a time, depending on the specific purpose for which we are using your data. If you'd like more information on the specific legal ground we are relying on, on occasions where we rely on more than one legal ground, please feel free to contact us.

Do we use Cookies?

Cookies help make our website work better for you, remembering your preferences and improving your experience. You can control cookie settings in your browser. Cookies make your browsing experience on our site as smooth as possible, because they remember your preferences.

Our website uses cookies to distinguish you from other users of our website. Please refer to our Cookie Policy to learn more.

Do we use your data for marketing purposes?

If we send you marketing communications and you no longer wish to receive them, you can opt out anytime by contacting us or clicking on the 'unsubscribe' button on our marketing communications. Our lawful ground of processing your personal data to send you marketing communications is either your consent or our legitimate interests (namely to grow our practice).

Do we use third-party links?

Our website might link to third-party websites, tools and apps. Clicking on these links may allow third parties to collect or share your data. We do not control said websites and are not responsible for said websites' privacy policies. When you leave our website, we encourage you to read the privacy policy of every website you visit.

Do we ever share your personal data?

We take your data's security seriously and only allow certain people to access it. We may share your personal data with the parties set out below for the purposes as stated further above.

- Service providers, acting as processors who provide IT and system administration services.
- Professional advisers including healthcare professionals, lawyers, bankers, auditors and insurers who provide consultancy, banking, legal, insurance and accounting services.
- As HCPC accredited clinician's, we are obliged to consult with another mental health professional for supervision purposes. This is to ensure we reflect and improve on our clinical skills. When discussing clients in supervision we only refer to clients by their first name and identifiable information is minimised.
- HM Revenue & Customs, regulators and other authorities who require reporting of processing activities in certain circumstances.
- Debt collection agencies in the event that payment is not received for services rendered. This will be done to recover any outstanding debts, and the debt collectors will process your data solely for this purpose.

Your legal team and case manager may request a summary of every therapy session and/or an assessment summary, progress reports and discharge summaries, which we will provide with your consent. You will be given the opportunity to read and consent to the content of these documents before they are shared and can request that information is not shared provided that information does not put yourself or others at risk of harm. If indicated, we will request your permission to send summary reports / letters to your GP or other medical professionals. We are obliged to share all risk-based information and where appropriate, will discuss this with you first.

All of the above third parties have a requirement to respect the security of your personal data. We do not permit them to use your personal data for their own purposes – they are only permitted to process your data for specified purposes in line with our instructions.

Confidentiality and Consent

The treatment you receive is confidential which means we will not share details of your treatment with other people without your explicit consent. The treating team and case manager share information relevant to your rehabilitation. We will share notes about the patient within our team and associates using a clinical shared note system (QuNote), ensuring that all practices are safe and GDPR-compliant. If there is anything you wish not to be shared outside the realms of one discipline, please discuss this with the treating therapist. There are circumstances under 'duty of care' in which health professionals are legally required to breach confidentiality and share information with outside agencies. This applies if we believe that failure to do so will result in harm to you or others. Specifically, this will apply if:

- ❖ we are concerned that you may hurt yourself or someone else
- ❖ we are concerned that you are vulnerable to being harmed by someone else,
- ❖ we believe you have not disclosed relevant information required by law that could affect your safety: at work; ability to drive; operate machinery; or ability to hold any type of license (e.g. pilot, firearms).

The services that we may contact could include your GP, Case Manager, Solicitor, Social Services, the Police or the DVLA. We will make all reasonable effort to discuss any concerns with you before contacting any services.

Child Protection. All healthcare professionals have a duty of care to protect children from potential harm. Any information that we receive, that may indicate the possibility that a child may be at risk of harm must be shared with Social Services and in some instances the Police. We will make all reasonable effort to discuss this with you if it arises, but we do not require your consent to proceed.

Do we use AI?

Artificial Intelligence (AI): AI refers to the use of computer systems, software, or applications that are designed to perform tasks that would normally require human intelligence. This includes, but

is not limited to, capabilities such as learning, reasoning, problem-solving, perception, language understanding, and interaction.

We may use AI tools to assist with the provision of our services, including [describe specific uses, e.g., data analysis, drafting documents, responding to enquiries]. Any AI tools we employ are used in compliance with applicable data protection laws, including the UK General Data Protection Regulation (UK GDPR).

When using AI tools, we ensure:

- Personal data is processed lawfully, fairly, and transparently.
- Data minimisation principles are upheld, meaning we only provide AI tools with the information strictly necessary for the intended purpose.
- Robust security measures are in place to protect your personal data during any processing involving AI tools.
- When using AI tools, we ensure that personal data is retained only for as long as necessary to fulfil the purposes outlined in our policy, after which it is securely deleted or anonymised.

We have listed below the specific AI tools we are using within our business, the purpose, the types of data we are collecting and our legal basis for this processing.

AI Tool Name	Purpose	Types of Data Used	Legal Basis for Processing
ChatGPT	Summarising research publications and sentence structure/clarity in reports. Creation of bespoke session resources.	None	N/A no client data included
Heidi Health	To summarise clinical notes for reports	None	N/A no client data included
Microsoft CoPilot	Summarising research publications and sentence structure/clarity in reports	None	N/A no client data included

For further enquiries on our AI usage or to exercise your rights, please contact us using the details provided in this policy.

Do we ever transfer your data internationally?

We may transfer your data outside of the United Kingdom/EEA, but only when we can be sure it is protected.

Many of our external third parties - including our cloud storage provider, email services, or video consultation platforms - are based outside the United Kingdom/EEA and so their processing of your personal data will involve a transfer of data outside the United Kingdom.

Whenever we transfer your personal data out of the United Kingdom, we make sure it is protected by at least implementing one of the following safeguards:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the United Kingdom
- Where we use certain service providers, we may use specific contracts approved by the UK Information Commissioner's Office and the European Commission which give personal data the same protection it has in Europe.

We also only utilise software that is GDPR-compliant.

Please contact us if you want further information on the specific process used by us when transferring your personal data out of the United Kingdom.

How secure is your data with us?

We have strong security measures in place to keep your personal information safe. Only authorised individuals who have a need to know are granted access to your data, such as our employees or trusted partners. They will process your data in accordance with our confidentiality terms.

Health professionals are required to keep a record of the treatment you receive at every visit or contact. This includes liaising with professionals within your team via telephone call, video call or email. We take notes during your appointment and these paper notes are either stored in a locked cabinet in accordance with GDPR guidance or shredded once transferred to our electronic notes system. All Arbor therapists are required to write in your shared electronic notes (accessible with a password known only to Arbor associates and administrative support) to ensure sharing of information within the clinical team.

Data submitted via our 'Make a Referral' form will be stored on our secure email system. Directors and administrative staff only will have access to this data.

Hard copies of documents delivered to Arbor's virtual address (Henleaze Business Centre, Harbury Road, Bristol, BS9 4PN) will be forwarded without being opened to Arbor's administrative team. The Henleaze Business Centre virtual office is managed by Virtually There.

In the rare circumstances that there is a personal data breach, we have procedures in place and will notify you, along with any applicable regulator, when we're legally required to.

What is our process for retaining your data?

We only keep your data as long as necessary for the reasons we collected it.

By law we have to keep medical information about patients for 7 years after treatment has finished. For any children we treat, we are obliged to retain the medical information until the child's 25th birthday, or seven years post-treatment – whichever is longer. By law we have to keep basic information about our clients (including contact, identity, financial and transaction data) for six years after they cease being patients for tax purposes.

For information that does not fall under the definition of basic, to determine the appropriate retention time, we look at what kind of data it is, how sensitive it is, the risks if it's misused, why we need it, and if there are other ways to achieve the same goals. We also consider applicable legal, regulatory, tax, accounting and other requirements.

What are your legal rights in relation to your data?

You have the following rights regarding your personal data:

Access: You can request a copy of the personal data we hold about you. This is known as a "data subject access request."

Correction: If the personal data we have about you is incomplete or incorrect, you can ask us to correct it.

Erasure: You can ask us to delete your personal data. It's important to note, however, that there might be legal reasons that prevent us from fulfilling this request. If such reasons exist, we will inform you when you make your request.

Objection: In certain situations, you have the right to object to the processing of your personal data.

Restriction of Processing: You can request that we restrict the processing of your personal data under specific circumstances.

Data Portability: You have the right to request the transfer of your personal data directly to you or to a third party of your choice.

Withdrawal of Consent: At any point where we rely on your consent to process your personal data, you have the right to withdraw this consent. Withdrawal of consent will not affect the legality of the processing done before the consent was withdrawn. Should you withdraw your consent, we might be unable to provide you with certain products or services. We will inform you if that is the case when you withdraw your consent.

If you wish to exercise any of the rights set out above, **please contact us.**

We won't charge any fees for you to request access to your personal data. However, a reasonable fee may be charged if your request is clearly unjustified, repetitive or excessive. We also reserve the right to not comply in this scenario. We try to respond to all legitimate requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

Changes and Contact

We regularly review our privacy policy. Please keep us updated if your personal data changes. If you have any questions or need to exercise your rights, just get in touch.

Thanks for reading our privacy policy. If you have any questions please don't hesitate to contact us.