PRIVACY NOTICE
THE LEE MEDICAL PRACTICE

BACKGROUND:

The Lee Medical Practice understands that your privacy is important to you and that you care about how your personal data is used. We respect and value the privacy of all of our patients and suppliers and will only collect and use personal data in ways that are described here, and in a way that is consistent with our obligations and your rights under the law.

1. **Information about Us**

The Lee Medical Practice, a partnership:

Blaire House, Denham Green Lane, Denham, Bucks UB9 5LQ

We do not have a data protection officer but Michele Lee, Partner is our lead and overseas all aspects relating to data protection

Email: office@leemedical.co.uk

Telephone number: 01895835144

2. **What Does This Notice Cover?**

This Privacy Information explains how we use your personal data: how it is collected, how it is held, and how it is processed. It also explains your rights under the law relating to your personal data.

3. **What is Personal Data?**

Personal data is defined by the General Data Protection Regulation (EU Regulation 2016/679) (the "GDPR") as 'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier'.

Personal data is, in simpler terms, any information about you that enables you to be identified. Personal data covers obvious information such as your name and contact details, but it also covers less obvious information such as identification numbers, electronic location data, and other online identifiers.

The personal data that we use is set out in Part 5, below.

4. **What Are My Rights?**

Under the GDPR, you have the following rights, which we will always work to uphold:

a) The right to be informed about our collection and use of your personal data. This Privacy Notice should tell you everything you need to know, but you can always contact us to find out more or to ask any questions using the details in Part 11.

b) The right to access the personal data we hold about you. Part 10 will tell you how to do this.

c) The right to have your personal data rectified if any of your personal data held by us is inaccurate or incomplete. Please contact us using the details in Part 11 to find out more.

d) The right to be forgotten, i.e. the right to ask us to delete or otherwise dispose of any of your personal data that we have. Please contact **us** using the details in Part 11 to find out more. This relates to any suppliers or any others, other than patients. Data collected at the Lee Medical Practice relating to patients is considered to be Special Category Data and therefore there is no absolute right to be forgotten. Patients can ask for their personal data to be erased but only when there is no compelling reason for its continued processing (see sections 15 & 18);

e) The right to restrict (i.e. prevent) the processing of your personal data.

f) The right to object to us using your personal data for a particular purpose or purposes.

g) The right to data portability. This means that, if you have provided personal data to us directly, we are using it with your consent or for the performance of a contract, and that data is processed using automated means, you can askus for a copy of that personal data to re-use with another service or business in many cases.

h) Rights relating to automated decision-making and profiling. We do not use your personal data in this way

i) For more information about our use of your personal data or exercising your rights as outlined above, please contact us using the details provided in Part 11.

Further information about your rights can also be obtained from the Information Commissioner's Office or your local Citizens Advice Bureau.

If you have any cause for complaint about **[**our**]** **OR [**my**]** use of your personal data, you have the right to lodge a complaint with the Information Commissioner's Office.

5. What Personal Data Do You Collect?

We may collect some or all of the following personal data (this may vary according to your relationship with us):

- Name;
- Date of birth;
- Gender;
- Address;
- Email address;
- Telephone number;
- Business name;
- Job title;
- Profession;
- Payment information;
- G.P.
- Other medical professionals who you are under
- Insurance companies if they are settling your account

- Referral information
- Any other further information as set out in our data protection policy

Your personal data may also be obtained from the following third parties:

- Hospital of referral
- Medical professional referrral

6. **How Do You Use My Personal Data?**

Under the GDPR, we must always have a lawful basis for using personal data. This may be because the data is necessary for our performance of a contract with you, because you have consented to our using of your personal data, or because it is in our legitimate business interests to use it. Your personal data will be used for the following purposes:

- As a supplier providing and managing your account.
- Communicating with you. This may include responding to emails or calls from you
- Supplying you with information by email **or** post that you have opted-in to (you may unsubscribe or opt-out at any time by contacting us

The following personal data relating to patients and staff may be collected, held, and processed by the Practice:

a) Name, address, date of birth telephone number and email address so that a patient can be easily identified, contacted directly and for identification for their G.P. and referring agencies. Information is kept on Practice Manager and in notes which are filed in a locked filing cabinet and in a locked office. In addition, a patient's name and date of birth will be held on medical equipment (including but not restricted to OCT machine, Visionix, Biometry and fields machine). The machines are password protected and where not (ie Visionix and fields machine) these machines will be kept in a locked room when not in use. The premises are secured by a monitored alarm system. Results from these machines will be kept in the patients notes which as described above are kept in a locked filing cabinet and in a locked office.

b) Referral letter and past medical history including medication taken for explanation and understanding of reason for patient's condition and reason for referral. Information is kept on Practice Manager and in notes which are filed in a locked filing cabinet and in a locked office

c) Assessment, operative notes, consent for relevant treatment, treatment notes and any medical test results for legal purposes to properly document the accurate management of a patient. The records held ensure the medical evaluation of the patient needs, assist in analyzing the treatment results, and to plan treatment protocols. It also helps in planning future medical care. Treatment notes identify what treatment has been carried out. Information is kept on Practice Manager and in notes which are filed in a locked filing cabinet and in a locked office

d) Insurance companies also require proper record keeping to prove the patient's demand for medical expenses. Information is kept on Practice Manager and in notes which are filed in a locked filing cabinet and in a locked office

e) Copies of assessment and reports will be sent to the patient, parent of the child who is under the age of 16, and with their permission to the referring

agency and G.P. A further copy of any report for paediatric patients will be sent to the parents if they wish to give a copy to any other agency (e.g. the school). The Practice will not send any copies directly to any agency without prior consent..

f) No records or patient information will be sent to any other body except for those listed above. In the event that a patient wishes their personal data and information to be sent to any other agencies then they will put this in writing to the practice secretary who with the agreement of the Practice Partner, send a hard copy to the agency or encrypted via email.

g) Account records of invoices and payments both for patients and suppliers will be kept on Practice Manager, Sage and Cardsave (part of world pay).These are kept in order to ensure correct accounting proceedures are carried out and for completing tax returns. Paper work relating to a patient's or supplier's account will be kept in files, in a locked office.

h) The practice has CCTV for security purposes only. There are 2 notices, one by the front door and the other by the back gate to inform those entering the premises that CCTV is present.

i) Data relating to staff members include

- Identification information relating to employees including, but not limited to, names and contact details;
- Equal opportunities monitoring information including age, gender, race, nationality and religion. **(**Such information shall be anonymised wherever possible**)**;
- Details of length of sick and annual leave;
- Employment records including, but not limited to, interview notes, curricula vitae, application forms, assessments, performance reviews and similar documents;
- Details of salaries including increases, bonuses, commission, overtime, benefits and expenses;
- Records of disciplinary matters including reports and warnings, both formal and informal;
- Details of grievances including documentary evidence, notes from interviews, procedures followed and outcomes;
- Bank account details in order for salary payment;

That data will be collected, held securely and processed in accordance with the data protection principles and with this Policy. The following data may be collected, held and processed by the Practice:

7. How Long Will You Keep My Personal Data?

The Practice shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. All patient notes will be digitally archived. For an adult patient this will be for 10 years after the last appointment/contact or if a patient has died or left the country. For children and young people records will be retained until the patient is 25 (or 26 if they are 17 when treatment ends) or eight years after their death, if sooner. When the data is no longer required, all reasonable steps will be taken to erase it without delay. All accountancy records will be kept for the

recommended HMRC guidelines after which time, all reasonable steps will be taken to erase them without delay

8. How and Where Do You Store or Transfer My Personal Data?

The Practice shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. We will only store or transfer your personal data in the UK. This means that it will be fully protected under the GDPR.]

The Practice shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

a) All information is stored on secured and encrypted systems

b) emails containing personal data must be encrypted using EGRESS.

c) Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely using a secure method.

d) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

e) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

f) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely on Practice Manager. The email itself should be deleted. All temporary files associated therewith should also be deleted;

g) Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data unless this is an approved safe haven (ie hospital pharmacy, theatres, outpatients, insurance companies, other medical practices);

h) Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient, referring agency or sent using the mail service.

i) No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Practice requires access to any personal data that they do not already have access to, such access should be formally requested from the Practice Partner and written confirmation given with a copy kept in a locked filing cabinet in the locked office.

j) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;

k) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Practice or not, without the written authorisation of the Practice Partner

l) Where an outside agency requests information on a patient (e.g. medical insurance company or another medical professional), then written consent of the patient must be shown and sent to the Practice. This will be scanned and kept on Practice Manager. A hard copy will be kept in their notes.

m) Personal data must be handled with care at all times and should not be left

unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;

n) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

o) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Practice or otherwise **(**without the formal written approval of the Practice Partner, the Lee Medical Practice) and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.

p) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Practice where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to the Practice that all suitable technical and organisational measures have been taken);

q) All personal data stored electronically should be backed up daily with backups stored off site. All backups should be encrypted by the service providers of the systems that are used by the Lee Medical Practice;

r) All electronic copies of personal data should be stored securely using passwords and the relevant system data encryption where available (some medical devices do not provide encryption eg Zeiss medical equipment but does provide password level of protection. Fields machine and Visionix do not have passwords but all these devices are securely stored);

s) All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by the Practice is designed to require such passwords;

t) Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Practice, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

u) No personal data held by the Practice is used for marketing purposes.

v) Where personal data is used for research purposes and audit, the patient will be asked to give written consent which will be kept on Practice Manager and a hard copy in their notes and no names or personal data will be used.

w) If any personal data is no longer required by the Practice, it should be securely deleted and disposed of by shredding or secure erase of electronic data; Old hard drives will be physically drilled to be destroyed.

x) Recordings from the CCTV systems are securely stored in a locked office and access is restricted to authorised personnel. Recordings are kept for 3 days after which time the recordings are recorded over. Appropriate security safeguards are in place to prevent interception and unauthorised access, either copying recordings or viewing. Any request from an individual or police for access to the CCTV recordings will be made to the Partner of the Practice.

9. Do You Share My Personal Data?

No personal data relating to suppliers is shared.

For patients your personal data may be shared with your GP and/or any professional that you inform us that you wish us to send reports to.

Hospitals will be informed of your personal data for clinics, operations and other proceedures

Insurance companies may be informed of your personal data provided you have given us consent to communicate with them

10. How Can I Access My Personal Data?

If you want to know what personal data we have about you, you can ask us for details of that personal data and for a copy of it (where any such personal data is held). This is known as a "subject access request". We always send a copy of your reports to you.

All subject access requests should be made in writing and sent to the email or postal addresses shown in Part 11.

There is not normally any charge for a subject access request. If your request is 'manifestly unfounded or excessive' (for example, if you make repetitive requests) a fee may be charged to cover administrative costs in responding.

We will respond to your subject access request within a month. Normally,we aim to provide a complete response, including a copy of your personal data within that time. In some cases, however, particularly if your request is more complex, more time may be required up to a maximum of three months from the date we receive your request. You will be kept fully informed of our progress.

11. How Do I Contact You?

To contact us about anything to do with your personal data and data protection, including to make a subject access request, please use the following details **[**(for the attention of Mrs Michele Lee MBE

Email address:michele@leemedical.co.uk

Telephone number: 01895 835144.

Postal Address: Blaire House, Denham Green Lane, Denham Bucks UB9 5LQ.

12. Changes to this Privacy Notice

We may change this Privacy Notice from time to time. This may be necessary, for example, if the law changes, or if we change our business in a way that affects personal data protection.

Any changes will be made available on our website www.dyspraxia-dcd.co.uk or www.nicholaslee.co.uk