NEWTON DRIVE HEALTH CENTRE

INFORMATION GOVERNANCE

Data Protection & GDPR Policy

1. Introduction. The Practice complies with the legal obligations of the Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('GDPR'). The Practice gathers and uses data about workers, employees and consultants, both to manage our relationships with these individuals and in the course of conducting our business.

This Data Protection Policy applies to current and former employees, workers, volunteers, consultants and apprentices ('data subjects').

The Practice is a 'data controller' for the purposes of these individuals' personal data, and is responsible for determining the purpose and means of the processing of that data.

In line with our Records Retention Policy and Computer and Data Security Procedure, the Practice has measures in place to protect the security of individuals' data. A copy of this can be obtained from the Practice Manager. Data will only be held for as long as is necessary for the purposes it has been collected.

This policy has been created to be fully compliant with GDPR and the 2018 Act. Where any conflict arises between those laws and this policy, the Practice will comply with the 2018 Act and the GDPR. This policy is separate from data subjects' contracts of employment (or contract for services) and can be amended by the Practice at any time.

2. The Six Data Protection Principles. The Practice processes personal data in accordance with the six Data Protection Principles for GDPR identified by the ICO, which means it will:

- Be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- Be processed fairly, lawfully and transparently;
- Be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- Be collected and processed only for specified, explicit and legitimate purposes;
- Not be kept for longer than is necessary for the purposes for which it is processed; and
- Be processed securely.

N.B It is a criminal offence if staff view any patient information without just cause and the practice has an obligation to report any such activity to the Information Commissioners Office (ICO)

3. Personal Data. Is defined as information relating to a living person ('data subject') that can be used to identify them on its own, OR in combination with other information likely to be collected by the Practice. This applies whether the information is stored physically, electronically, or in any other format.

It **does not** include anonymised data, but **does** include any expression of opinion about the person, or any indication of the intentions of the Practice or others, in respect to that individual. Personal data might be provided to the Practice by the individual, or someone else (such as a previous employer or their GP), or it could be created by the Practice. It could be provided or created as part of the recruitment process; in the course of the contract of employment (or services); or after its termination.

To view the types of personal data and information that the Practice may collect about staff please view the 'Privacy Notice – Staff'

4. **Special Categories of Personal Data.** These comprise personal data consisting of information relating to:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic or biometric data;
- Health;
- Sex life and sexual orientation; and
- Criminal convictions and offences.

The Practice may hold and use any of these special categories of your personal data in accordance with the law.

5. **Processing Personal Data**. 'Processing' means any operation which is performed on personal data such as:

- Disclosure by transmission, dissemination or otherwise making available;
- Alignment or combination;
- Collection, recording, organisation, structuring or storage (e.g. within a filing system);
- Adaption or alteration;
- Retrieval, consultation or use; and
- Restriction, destruction or erasure.

The Practice will process individuals' personal data (including special categories of personal data) in accordance with the obligations prescribed under the 2018 Act, including:

- Performing the contract of employment (or services) between the Practice and the individual;
- Complying with any legal obligation; or;
- If it is necessary for the Practice's legitimate interests (or for the legitimate interests of someone else). The Practice can only do this in circumstances where the individual's interests and rights do not override those of the Practice (or their own). Individuals have the right to challenge the Practice's legitimate interests and request that this processing be halted.

The Practice may process individuals' personal data for these purposes without your knowledge or consent. The Practice will not use your personal data for an unrelated purpose without informing you about it and the legal basis for processing it.

Please note that if individuals opt not to provide the Practice with some personal data, the Practice may be unable to carry out certain parts of the contract between us, e.g. the Practice needs staff members' bank account details in order to pay them.

6. **When the Practice Might Process Your Personal Data**. The Practice is required to process individuals' personal data in various situations during their recruitment, employment (or engagement) and even following termination of their employment (or engagement) for reasons including but not limited to:

- Deciding how much to pay staff, and other terms of their contract with the Practice;
- Ensuring they have the legal right to work for the Practice;
- Carrying out the contract between the Practice and the individual including, where relevant, its termination;
- Carrying out a disciplinary or grievance investigation or procedure in relation to them or someone else;
- Monitoring and protecting the security (including network security) of the Practice, of the individual, other staff, patients and others;
- Paying tax and national insurance;
- Providing a reference upon request from another employer;
- Preventing and detecting fraud or other criminal offences;
- and any other reason which we may notify you of from time to time.

The Practice may process special categories of personal data to use information in relation to your:

- race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
- sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety;

The Practice does not take automated decisions about you using your personal data or use profiling in relation to you. The Practice will only process special categories of individuals' personal data in certain situations in accordance with the law e.g. with their explicit consent. If the Practice requests consent to process a special category of an individuals' personal data, the reasons for the request will be explained. Individuals do not need to consent and can withdraw consent later if they choose by contacting the Practice Manager.

The Practice does not need consent to process special categories of individuals' personal data when it is processed it for the following purposes:

- Where it is necessary for carrying out rights and obligations under employment law;
- Where it is necessary to protect individuals' vital interests or those of another person where one or both parties are physically or legally incapable of giving consent;
- Where the individual has made the data public;
- Where processing is necessary for the establishment, exercise or defence of legal claims; and
- Where processing is necessary for the purposes of occupational medicine or for the assessment of the individuals' working capacity.

All employment checks, including those for criminal records, will be carried out in line with the guidance from NHS Employers, available at: www.nhsemployers.org/your-workforce/recruit/employment-checks/criminal-record-check.

7. Sharing Your Personal Data. Sometimes the Practice might share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests. We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

The Practice ***does not*** send your personal data outside the European Economic Area. If this changes you will be notified and the protections in place to protect the security of your data will be explained.

8. Processing Personal Data for the Practice. All staff who work for, or on behalf of, the Practice has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this Data Protection policy and the Practice's Records Retention Policy and Computer and Data Security Procedure.

The Practice's Data Protection Officer/Data Protection Manager is responsible for reviewing this policy and updating the Managing Partners on the Practice's responsibilities for data protection, and any risks in relation to the processing of data. Any questions related to this policy or data protection should be directed to the Practice Manager.

All members of staff must follow these rules:

- Staff must only access personal data covered by this policy if needed for purposes necessary to their job, or on behalf of the Practice, and only if they are authorised to do so. The data must only be utilised for the specified lawful purpose for which it was obtained.
- Personal data must be kept secure and not shared with unauthorised people.
- Personal data that is accessed, stored and collected for working purposes must be regularly reviewed and updated. This includes informing the Practice of changes to your personal contact details.
- Do not make unnecessary copies of personal data. Any unused copies must be kept safe before being securely disposed of.
- Use strong passwords and lock computer screens when not at your workstation.
- Where suitable, anonymise data or use separate keys/codes so that the data subject cannot be identified.
- **Under no circumstances** save personal data to personal computers or other devices.
- Personal data should never be transferred outside the European Economic Area except to comply with the law and with the authorisation of the Data Protection Officer.
- Lock drawers and filing cabinets and do not leave paper with personal data unattended.
- Do not remove personal data from the Practice's premises without authorisation from your line manager or Data Protection Officer / Practice Manager.
- Personal data should be shredded and securely disposed of when it is no longer needed.

Please contact our Data Protection Officer/Data Protection Manager if you have any questions about data protection, or if you become aware of any potential improvements or vulnerabilities in data protection or data security that the Practice can improve upon.

Any deliberate or negligent breach of this policy may result in disciplinary action being taken in accordance with the Practice's Disciplinary Procedure. It is a criminal offence to conceal or destroy personal data which is part of a Subject Access Request. This conduct would be regarded as gross misconduct under the Practice's Disciplinary Procedure, which could result in dismissal.

9. Handling Data Breaches. The Practice has robust measures in place to minimise and prevent data breaches from occurring. Should a breach of personal data occur, the Practice will make note of the relevant details and circumstances, and keep evidence related to that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then the Practice will notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach you must contact your line manager or Practice Manager immediately and retain any related evidence to the breach that you may have.

10. Subject Access Requests. Data subjects can make a Subject Access Request ('SAR') to access the information the Practice holds about them. **This request must be made in writing**. If you receive a SAR you should forward it immediately to the Practice Secretary, who will prepare a response.

If you wish to make a SAR in relation to your own personal data this should be made in writing to the Practice Manager. The Practice will respond within one month unless the request is complex or numerous – if this is the case, then the Practice will need more time to complete the request, and can extend the response period by a further two months.

A Subject Access Request does not incur a fee, however, if the request is deemed to be manifestly unfounded or excessive then Practice is entitled to charge a reasonable administrative fee, or refuse to respond to the request.

11. Data Subjects' Rights. In most situations the Practice will not rely on your consent as a lawful ground to process your data. If the Practice does request your consent to the processing of your personal data for a specific purpose, you have the right to decline or withdraw your consent at a later time. To withdraw consent, you should contact the Practice Manager.

Data subjects have the right to information about what personal data the Practice processes, how it is processed and on what basis. They have the right to:

- Access their personal data via a Subject Access Request.
- Correct any inaccuracies in their personal data. To do so please contact the Practice Manager.
- Request that we erase their personal data in the case that the Practice was not entitled under the law to process it, or the data is no longer needed for the purpose it was collected. In this case please contact the Practice Manager.
- Object to data processing where the Practice is relying on a legitimate interest to do so and the data subject contends that their rights and interests outweigh those of the Practice and wish us to stop.
- Object if the Practice processes their personal data for the purposes of direct marketing.
- Receive a copy of their personal data and transfer their personal data to another data controller. The Practice will not charge for this and will in most cases aim to do this within one month.
- With some exceptions, they have the right not to be exposed or subjected to automated decision-making.
- Be notified of a data security breach (within the appropriate timescales) concerning their personal data.

If you have a complaint about how your data is processed that cannot be resolved with the Practice, you have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office at www.ico.org.uk. Where your personal data is being corrected or erased, or the Practice is contesting the lawfulness of the processing, you can apply for its use to be restricted while the application is made. In this case please contact the Practice Manager.

12. Resources

Information Commissioner's Office website - www.ico.org.uk
NHS Employers guidance on criminal checks - www.nhsemployers.org/your-workforce/recruit/employment-checks/criminal-record-check
Records Retention Policy
Computer and Data Security Procedure