WETMORE ROAD SURGERY

Data Security & Protection Policy

Document Control

A. Confidentiality Notice

This document and the information contained therein is the property of WETMORE ROAD SURGERY.

This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from WETMORE ROAD SURGERY.

B. Document Details

Classification:	Information Governance
Relevant to	All Staff
Organisation:	WETMORE ROAD SURGERY
Version	3
Date Approved	March 2013
Last Review	June 2021
Next Review	June 2022

C. Document Revision and Approval History

Version	Date	Version Created By:	Version Approved By:	Comments
2	Mar 2014	RP/AW	RP/AW	
2	Feb 2017		RP/AW	Reviewed – No Amendment
2	Dec 2017		RP/AW	Reviewed – No Amendment
3	Feb 2019		RP/AW	References to GDPR included
3	Dec 2019		RP/AW	Included details on DPA Policy
3	Jun 2021	RP/AW	RP/AW	Full Rewrite

Overview

1. The Practice takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the EU General Data Protection Regulation ("GDPR") in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

2. This policy applies to current and former directors, Partners, employees, apprentices and consultants. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to your data.

3. The Practice has measures in place to protect the security of your data in accordance with our various data security policies. We will only hold data for as long as necessary for the purposes for which we collected it.

4. The Practice is a 'data controller' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

5. This policy explains how the Practice will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Practice.

6. This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by the Practice at any time. It is intended that this policy is fully compliant with the GDPR and will be updated as required upon the enactment of the DPA. If any conflict arises between the law and this policy, the Practice intends to comply with the Law.

Data Protection Principles

7. Personal data must be processed in accordance with six 'Data Protection Principles.' It must:

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

8. We are accountable for these principles and must be able to show that we are compliant.

How we define personal data

9. 'Personal data' means information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information

which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

10. This policy applies to all personal data whether it is stored electronically or on paper.

11. This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

12. We will collect and use the following types of personal data about you:

    - recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
    - your contact details and date of birth;
    - the contact details for your emergency contacts;
    - your gender;
    - your marital status and family details;
    - information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
    - your bank details and information in relation to your tax status including your national insurance number;
    - your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us;
    - information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
    - information relating to your performance and behaviour at work;
    - training records;
    - immunisation records if appropriate for your role;
    - your images (whether captured on CCTV, by photograph or video);
    - any other category of personal data which we may notify you of from time to time.

How we define special categories of personal data

13. 'Special categories of personal data' are types of personal data consisting of information as to:

    - your racial or ethnic origin;
    - your political opinions;
    - your religious or philosophical beliefs;
    - your trade union membership;
    - your genetic or biometric data;
    - your health;
    - your sex life and sexual orientation; and
    - any criminal convictions and offences.

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

How we define processing

15. 'Processing' means any operation which is performed on personal data such as:

    - collection, recording, organisation, structuring or storage;
    - adaption or alteration;
    - retrieval, consultation or use;
    - disclosure by transmission, dissemination or otherwise making available;
    - alignment or combination; and
    - restriction, destruction or erasure.

16. This includes processing personal data which forms part of a filing system and any automated processing.

How will we process your personal data?

17. The Practice will process your personal data (including special categories of personal data) in accordance with our obligations under the law.

18. We will use your personal data for:

    - performing the contract of employment (or services) between us;
    - complying with any legal obligation; or
    - if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing.

19. We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

20. If you choose not to provide us with certain personal data you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

21. Where your choice not to give us certain personal data means we are unable to comply with our legal obligations or the terms of our contract with you, we may be obliged to terminate your employment (or engagement).

Examples of when we might process your personal data

22. We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

23. For example, (and see below for the meaning of the asterisks): -

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and the other terms of your contract with us;
- to check you have the legal right to work for us;
- to carry out the contract between us including where relevant, its termination;
- training you and reviewing your performance*;
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct*;
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability*;
- to monitor diversity and equal opportunities*;
- to monitor and protect the security (including network security) of the Practice, of you, our other staff, customers and others;
- to monitor and protect the health and safety of you, our other staff, customers and third parties*;
- to pay you and provide pension and other benefits in accordance with the contract between us*;
- paying tax and national insurance;
- to provide a reference upon request from another employer;
- monitoring compliance by you, us and others with our policies and our contractual obligations*;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us*;
- to answer questions from insurers in respect of any insurance policies which relate to you*;
- running our business and planning for the future;
- the prevention and detection of fraud or other criminal offences;
- to defend the Practice in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*;
- for any other reason which we may notify you of from time to time.

24. We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request.

25. We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do: -

- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;

- where you have 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 your working capacity.

26. If you have criminal convictions that are relevant to our employment of engagement of you, we will record this information for our own legitimate interests and to enable us to answer questions from our regulators and other entitled authorities.

27. We might process special categories of your personal data for the purposes set out in paragraph 23. In particular, we will use information in relation to: -

    - your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
    - your 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; and

28. We do not take automated decisions about you using your personal data or use profiling in relation to you.

Sharing your personal data

29. Sometimes we 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.

30. 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.

31. The third parties we use who may hold personal data about you are: -

    - [payroll company]
    - Pension provider]

32. We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

Retention of staff information post-employment

33. After you have left the Practice, we will retain the information we hold about you for a period of six years to enable us to comply with our legal obligations in respect of, for example, HMRC and the Department of Work and Pensions. We will also retain it to enable us to deal with any issues that arise relating to your employment after you have left. This is in our own legitimate interests.

How should you process personal data for the Practice?

34. Everyone who works for, or on behalf of, the Practice has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and other data protection policies.

35. The Practice's Data Protection Officer/Data Protection Manager is Mr Rob Paton who is responsible for reviewing this policy and updating the Board of Directors on the Practice's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

36. You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of, the Practice and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

37. You should not share personal data informally.

38. You should keep personal data secure and not share it with unauthorised people.

39. You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

40. You should not make unnecessary copies of personal data and should keep, and dispose of, any copies securely.

41. You should use strong passwords in accordance with our Data Security and Password Policy.

42. Consideration should always be given to encrypting personal data before transmitting out to a recipient outside our Practice.

43. Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

44. Do not save personal data to your own personal computers or other devices.

45. Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Data Protection Officer/Data Protection Manager.

46. You should lock drawers and filing cabinets where possible. Do not leave paper with personal data lying about.

47. You should not take personal data away from Practice's premises without authorisation.

48. Printed personal data should be shredded and disposed of securely when you have finished with it.

49. You should ask for help from the Practice Manager if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

50. Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

51. It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

How to deal with data breaches

52. We have robust measures in place to minimise and prevent data breaches from taking place, including a Data Breach Policy and Data Breach Register. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours.

Subject access requests

53. Data subjects can make a 'subject access request' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to the practice manager who will coordinate a response.

54. If you would like to make a SAR in relation to your own personal data you should make this in writing to the Data Protection Officer/Data Protection Manager. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

55. There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

56. You have the right to information about what personal data we process, how and on what basis as set out in this policy.

57. You have the right to access your own personal data by way of a subject access request (see above).

58. You can correct any inaccuracies in your personal data. To do you should contact the Practice Manager.

59. You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact the Practice Manager.

60. While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact the Practice Manager.

61. You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

62. You have the right to object if we process your personal data for the purposes of direct marketing.

63. With some exceptions, you have the right not to be subjected to automated decision-making.

64. You have the right to be notified of a data security breach concerning your personal data, unless the breach is trivial.

65. In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the Data Protection Officer/Data Protection Manager.

66. You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.