# Data protection policy

Introduction: All organisations that process personal data are required to comply with data protection legislation. This includes in particular the Data Protection Act 1998 (or its successor) and the EU General Data Protection Regulation (together the 'Data Protector Laws'). The Data Protector Laws give individuals (known as 'data subjects') certain rights over their personal data whilst imposing certain obligations on the organisations that process their data. As a business the Practice collects and processes both personal data and sensitive personal data. It is required to do so to comply with other legislation. It is also required to keep this data for different periods depending on the nature of the data. This policy sets out how the Practice implements the Data Protection Laws. It should be read in conjunction with the Data Protection Procedure

Data protection policy: Definitions In this policy the following terms have the following meanings: 'consent' means any freely given, specific, informed and unambiguous indication of an individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her; 'data controller' means an individual or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data; 'data processor' means an individual or organisation which processes personal data on behalf of the data controller; 'personal data' means any information relating to an individual who can be identified, such as by a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data; 'processing' means any operation or set of operations performed on personal data, such as collection, recording, organisation, structuring, storage (including archiving), adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements; 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to an individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual; 'sensitive personal data' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning health, an individual's sex life or sexual orientation and an individual's criminal convictions. For the purposes of this policy we use the term 'personal data' to include 'sensitive personal data' except where we specifically need to refer to sensitive personal data. 'Supervisory authority' means an independent public authority which is responsible for monitoring the application of data protection. In the UK the supervisory authority is the Information Commissioner's Office (ICO).

Data protection policy: Data processing under the Data Protection Laws The Practice processes personal data in relation to its own staff, work-seekers, DBS applicants and patients and is a data controller for the purposes of the Data Protection Laws.

The Practice ICO registration number is: **Z8664962.**

The Practice may hold personal data on individuals for the following purposes: Staff administration; Advertising, marketing and public relations; DBS Checks, Accounts, Payroll and records; Administration and processing of users' personal data for the purposes of supplying services; 1. The data protection principles The Data Protection Laws require the Practice acting as either data controller or data processor to process data in accordance with the principles of data protection. These require that personal data is: 1. Processed lawfully, fairly and in a transparent manner; 2. Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes; 3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; 4. Accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; 5. Kept for no longer than is necessary for the purposes for which the personal data are processed; 6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and that 7. The data controller shall be responsible for, and be able to demonstrate, compliance with the principles. Legal bases for processing. The Practice will only process personal data where it has a legal basis for doing so (see Annex A).Where the Practice does not have a legal reason for processing personal data any processing will be a breach of the Data Protection Laws. The Practice will review the personal data it holds on a regular basis to ensure it is being lawfully processed and it is accurate, relevant and up to date. Before transferring personal data to any third party (such as past, current or prospective employers, suppliers, customers and clients, delivery companies, intermediaries such as umbrella companies, persons making an enquiry or complaint and any other third party (such as software solutions providers and back office support)), the Practice will establish that it has a legal reason for making the transfer.

Data protection policy: Data processing under the Data Protection Laws 3. Privacy by design and by default. The Practice has implemented measures and procedures that adequately protect the privacy of individuals and ensures that data protection is integral to all processing activities. This includes implementing measures such as: data minimisation (i.e. not keeping data for longer than is necessary); pseudonymisation; anonymization; cyber security; encryption. For further information please refer to the Practice's Information Security Policy.

Data protection policy: Rights of the individual The Practice shall provide any information relating to data processing to an individual in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. The Practice may provide this information orally if requested to do so by the individual. 1. Privacy notices. Where the Practice collects personal data from the individual, the Practice will give the individual a privacy notice at the time when it first obtains the personal data. Where the Practice collects personal data other than from the individual directly, it will give the individual a privacy notice within a reasonable period a tier obtaining the personal data, but at the latest within one month. If the Practice intends to disclose the personal data to a third party then the privacy notice will be issued when the personal data are first disclosed (if not issued sooner). Where the Practice intends to further process the personal data for a purpose other than that for which the data was initially collected, the Practice will give the individual information on that other purpose and any relevant further information before it does the further processing. 2. Subject access requests. The individual is entitled to access their personal data on request from the data controller. 3. Rectification: The individual or another data controller at the individual's request, has the right to ask the Practice to rectify any inaccurate or incomplete personal data concerning an individual.

If the Practice has given the personal data to any third parties it will tell those third parties that it has received a request to rectify the personal data unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold – however the Practice will not be in a position to audit those third parties to ensure that the rectification has occurred.

4. Erasure - The individual or another data controller at the individual's request, has the right to ask the Practice to erase an individual's personal data. If the Practice receives a request to erase it will ask the individual if s/he wants his personal data to be removed entirely or whether s/he is happy for his or her details to be kept on a list of individuals who do not want to be contacted in the future (for a specified period or otherwise). The Practice cannot keep a record of individuals whose data it has erased so the individual may be contacted again by the Practice should the Practice come into possession of the individual's personal data at a later date. If the Practice has made the data public, it shall take reasonable steps to inform other data controllers and data processors processing the personal data to erase the personal data, taking into account available technology and the cost of implementation. If the Practice has given the personal data to any third parties it will tell those third parties that it has received a request to erase the personal data, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold – however the Practice will not be in a position to audit those third parties to ensure that the rectification has occurred. Data protection policy: Rights of the individual 5. Restriction of processing. The individual or a data controller at the individual's request, has the right to ask the Practice to restrict its processing of an individual's personal data where: The individual challenges the accuracy of the personal data; The processing is unlawful and the individual opposes its erasure; The Practice no longer needs the personal data for the purposes of the processing, but the personal data is required for the establishment, exercise or defence of legal claims; or The individual has objected to processing (on the grounds of a public interest or legitimate interest) pending the verification whether the legitimate grounds of the Practice override those of the individual. If the Practice has given the personal data to any third parties it will tell those third parties that it has received a request to restrict the personal data, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold – however the Practice will not be in a position to audit those third parties to ensure that the rectification has occurred. 6. Data portability. The individual shall have the right to receive personal data concerning him or her, which he or she has provided to the Practice, in a structured, commonly used and machine-readable format and have the right to transmit those data to another data controller in circumstances where: The processing is based on the individual's consent or a contract; and The processing is carried out by automated means. Where feasible, the Practice will send the personal data to a named third party on the individual's request. 7. Object to processing. The individual has the right to object to their personal data being processed based on a public interest or a legitimate interest. The individual will also be able to object to the profiling of their data based on a public interest or a legitimate interest. The Practice shall cease processing unless it has compelling legitimate grounds to continue to process the personal data which override the individual's interests, rights and freedoms or for the establishment, exercise or defence of legal claims. The individual has the right to object to their personal data for direct marketing. Please refer to the Practice's Marketing Policy for further information. 8. Enforcement of rights. All requests regarding individual rights should be sent to the Practice. The Practice shall act upon any subject access request, or any request relating to rectification, erasure, restriction, data portability or objection or automated decision making processes or profiling within one month of receipt of the request. The Practice may extend this period for two further months where necessary, taking into account the complexity and the number of requests.

Data protection policy: Rights of the individual Where the Practice considers that a request under this section is manifestly unfounded or excessive due to the request's repetitive nature the Practice may either refuse to act on the request or may charge a reasonable fee taking into account the administrative costs involved.9.Automated decision making The Practice will not subject individuals to decisions based on automated processing that produce a legal effect or a similarly significant effect on the individual, except where the automated decision:•Is necessary for the entering into or performance of a contract between the data controller and the individual; Is authorised by law; or The individual has given their explicit consent. The Practice will not carry out any automated decision-making or profiling using the personal data of a child.

Data protection policy: Personal data breaches Reporting personal data breaches. All data breaches should be referred to Dr Gordon.

Personal data breaches where the Practice is the data controller: Where the Practice establishes that a personal data breach has taken place, the Practice will take steps to contain and recover the breach. Where a personal data breach is likely to result in a risk to the rights and freedoms of any individual the Practice will notify the ICO. Where the personal data breach happens outside the UK, the Practice shall alert the relevant supervisory authority for data breaches in the effected jurisdiction. 2. Personal data breaches where the Practice is the data processor: The Practice will alert the relevant data controller as to the personal data breach as soon as they are aware of the breach. 3.Communicating personal data breaches to individuals. Where the Practice has identified a personal data breach resulting in a high risk to the rights and freedoms of any individual, the Practice shall tell all affected individuals without undue delay. The Practice will not be required to tell individuals about the personal data breach where: The Practice has implemented appropriate technical and organisational protection measures to the personal data affected by the breach, in particular to make the personal data unintelligible to any person who is not authorised to access it, such as encryption.•The Practice has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialise. It would involve disproportionate effort to tell all affected individuals. Instead, the Practice shall make a public communication or similar measure to tell all affected individuals.© Personnel Ltd. 2018

Data protection policy: The Human Rights Act 1998All individuals have the following rights under the Human Rights Act 1998 (HRA) and in dealing with personal data these should be respected at all times: Right to respect for private and family life (Article 8). Freedom of thought, belief and religion (Article 9). Freedom of expression (Article 10). Freedom of assembly and association (Article 11). Protection from discrimination in respect of rights and freedoms under the HRA (Article 14).

## PRIVACY POLICY BACKGROUND:

The St Peters Dental 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 everyone who visits our website, 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. Please read this Privacy Policy carefully and ensure that you understand it. Your acceptance of this. 4.What is Personal Data? Personal data is defined by the General Data Protection Regulation (EU Regulation2016/679) (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. 5. 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 Policy should tell you everything you need to know. b) The right to access the personal data we hold about you. Part 13 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 Part15 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 15 to find out more. 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 am using it with your consent or for the performance of a contract, and that data is processed

using automated means, you can ask us 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. 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 15. 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 use of your personal data, you have the right to lodge a complaint with the Information Commissioner's Office. 6. What Data Do We Collect? Depending upon your use of our website, we may collect some or all of the following personal and non-personal data (please also see Part 14 on Our use of Cookies and similar technologies):

•Name; •Date of birth; •Gender;•Address; •Email address; •Telephone number; •Business name; •Job title; •Profession; •Employment History; •Information about your preferences and interests

7. 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 use of your personal data, or because it is in our legitimate business interests to use it. Your personal data may be used for the following purposes: Providing and managing your Account; Providing and managing your access to our website; Personalising and tailoring your experience on our website; Supplying our products and/or services to you. Your personal details are required in order for us to enter into a contract with you.

Personalising and tailoring our products and services for you. Communicating with you. This may include responding to emails or calls from you. Supplying you with information by email and/or post that you have opted-in to (you may unsubscribe or opt-out at any time by logging in and changing your account preferences). Finding work and/or providing employment services for/to you. Analysing your use of our website and gathering feedback to enable us to continually improve our website and your user experience. With your permission and/or where permitted by law, we may also use your personal data for marketing purposes, which may include contacting you by email and/or telephone and/or text message and/or post with information, news, and offers on our products and/or services. You will not be sent any unlawful marketing or spam. we will always work to fully protect your rights and comply with Our obligations under the GDPR and the Privacy and Electronic Communications.