

# The Martock Dental Practice



## Privacy Policy

---

At The Martock Dental Practice we are dedicated to safeguarding and preserving your privacy when you visit the practice or communicate with us electronically in accordance with the GDPR (general data protection regulation). We will ensure that any personal information we hold about you is processed fairly and lawfully.

The Data Protection Officer for the practice is Fiona Head alongside Jeremy Hill

This privacy policy provides an explanation as to what happens with your personal data that you provide, or that we collect from you.

### Personal Data we may hold

To provide you with a high standard of dental care, we must keep comprehensive and accurate personal data about you. Personal information is information about you which can be identified, such as your name and contact details. And more sensitive information would be details about your medical health, and dental care you have received.

By providing us with your data and/or information, or by using our practice website or other online platforms, you consent to the use of your data and information as described or referred to in this privacy policy.

If any changes are made to how we process personal information, we will update our policy immediately and make this available on our website, so please check regularly for updates.

### Confidential and Medical Information

The confidentiality of your personal information is of paramount importance to The Martock Dental Practice and we comply with UK data protection law and all the applicable medical confidentiality guidelines issued by professional bodies such as General Dental and the British Dental Association.

Your confidential medical information will only be disclosed to those involved in your treatment or care, or in accordance with UK law and guidelines for professional bodies, or for the purposes of clinical audit (unless you withdraw consent). If you receive services from The Martock Dental Practice and that service transfers to another provider, we may share your personal and confidential medical information with the new provider.

### Securing Information

We are committed to keeping your personal information secure. We have put in place physical, electronic and operational procedures intended to safeguard the information we collect. All our staff have a legal duty to respect the confidentiality of your information, and access to your records is restricted only to those who have reasonable need to access it.

When using our practice website, if the URL of a web page starts with HTTPS, or you see a locked/green padlock symbol, your data should be encrypted when it is sent from your computer to our server. However, we cannot ensure the security of your data when it is being transmitted to our website. All transmission of personal information and other data is done at your own risk.

Information submitted to us through a website is normally unprotected until it reaches us. In addition, users are also requested not to send confidential details or credit card numbers, for example, by email.

### **What personal data that we hold includes:**

- Personal details such as your date of birth, NHS number, address, telephone number and your general medical practitioner
- Your past and current medical and dental health
- Radiographs, clinical photographs and study models
- Information about the treatment that we have provided or propose to provide and its cost
- Notes of conversations about your care
- Details of services you have received
- Records of consent to treatment
- Details of any contact we have had with you
- Patient experience feedback and treatment outcome information you may provide
- Correspondence with other health care professionals relating to you, for example in the hospital or community services.
- Information about any complaints or incidents
- Information from customer surveys

### **When we collect information**

Information about you is collected when:

- you use our services
- you submit a query to us, for example by email, telephone or social media, including where you reference Martock Dental Practice in a public social media post

We may also collect personal information about you from other people when:

- we liaise with your family, employer, health professional or other treatment or benefit provider. We may only share information in this way where you have provided your consent or in circumstances where you are incapable of giving consent, or we are unable or it is not reasonable to seek your permission, or we are required to by law or in accordance with guidance from professional bodies

### **Using your information**

We use your personal information to provide you with our services, and to improve and extend our services. This may include:

- responding to your queries
- supporting your medical treatment or care and other benefits
- internal record keeping and administration

- responding to requests where we have a legal or regulatory obligation to do so
- checking the accuracy of information about you, and the quality of your treatment or care, including auditing medical and billing information
- assessing the type and quality of care you have received and any concerns or complaints you raise, so that these can be properly investigated
- using your contact information to send you service related information
- using your contact information to send promotional material about new products, special offers or other information we think you may find interesting (see 'Keeping you informed' below for more information)
- NHS payment authorities
- using your contact information to give you an opportunity to complete a customer satisfaction survey

## Sharing Information

Martock Dental Practice works with other individuals and organisations to provide our services to you, and this may involve them handling your personal information. In that case we ensure that the confidentiality and security of your personal information is protected by contractual restrictions and service monitoring.

We do not share your personal information with anyone outside of the Martock Dental Practice to use for their own purposes, except:

- when we have your permission
- when we are permitted or obliged to do so by law. For example, we are required to provide information to organisations such as the National Registries (e.g. The Cancer Registry) and to notify the government of certain infectious diseases such as TB and meningitis (but not HIV/Aids)
- to protect the rights, property, or safety of Martock Dental Practice, our customers, or others
- in order to detect, prevent and help with the prosecution of financial crime. For example we may share information with fraud prevention or law enforcement agencies, and other organisations. If we suspect fraudulent activity we may inform the person or organisation who administers or funds your Bupa services.
- if there are other exceptional circumstances, and we are unable or it is not appropriate to seek your permission.

## Personal Privacy Rights

Under GDPR, all individuals who have personal data held about them have the following personal privacy rights:

- Right to subject access
- Right to have inaccuracies deleted
- Right to have information erased
- Right to object to direct marketing
- Right to restrict the processing of their information, including automated decision-making
- Right to data portability

## Automated Decision Making

This includes all decisions made without human intervention e.g. email reminders to book an appointment or text or email reminders of appointments, direct marketing i.e. all decisions that are taken automatically.

## Data Portability

The ability to take personal data elsewhere e.g. to another dental practice or employer.

## Legal Basis for Processing Data

There are six legal bases for processing personal data and we are required to be able to justify and articulate the legal basis on which we collect and process all personal data that we hold. We must also document the legal basis on which we collect and process all personal data that we hold.

Legal basis for sharing this information
A – Consent: the individual has given clear consent for specific purpose
B – Contract: processing is necessary for a contract with an individual
C – Legal Obligation: processing is necessary for you to comply with the law
D – Vital Interests: the processing to protect someone’s life
E – Public task: the processing is necessary for you to perform a task in the public interest or in your official functions, and the task or function has a clear basis in law
F – Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests.

## Retaining information

We will retain your dental records while you are a practice patient and after you cease to be a patient, for at least eleven years or, for children, until age of 25, whichever is the longer.

## Keeping you informed

The Martock Dental Practice would like to keep you informed of our products and services that we consider may be of interest to you (via mail, email, phone or SMS). When we collect your information, we will ask you if you would like us to keep you updated in this way. We may use your personal information to:

- decide which services we think are relevant to you
- decide which media, including social media platforms, would best be utilised to reach the customers who wish to receive marketing materials
- contact you with details of our products and services, including displaying interest-based adverts via social media

If you do not wish to receive marketing information about our products and services, or at any time you change your mind about receiving these messages, please contact our receptionist and your details will be removed.

## Security of information

Personal data about you is held in the practice computer system and/or in a manual filing system. The information is not accessible to the public; only authorised members of staff have access to it. Staff have been given training in their legal responsibilities under the Data Protection Act and practical procedures for maintaining confidentiality.

We take precautions to keep the practice premises, filing systems and computers physically secure. Our computer system has secure audit trails and we back-up information routinely. We use cloud computing facilities for the storage and processing of some of your data. The practice has a rigorous service level agreement with our cloud provider to ensure that all our obligations in this policy are fulfilled and that your information is secure.

## Risk Management

We have reviewed and enhanced our data protection risk management processes and recorded our actions on our GDPR risk assessment template. We undertake annual data protection risk assessments and follow up to ensure actions have been completed.

GDPR compliance is discussed at our practice meetings monthly and actions arising are recorded and followed up.

We have a clear, robust, binding written contract with our practice management software suppliers SOE (exact) and all other external data processors see extensive 3<sup>rd</sup> party processors list to ensure they comply with GDPR.

## Risk management protocols

All team members must ensure that they:

- Do not leave people's information out on their desk
- Lock filing cabinets when the practice is unattended
- Do not leave data displayed on screen (use a screensaver)
- Ensure that their PC screen cannot be seen by anyone who is not entitled to see it
- Do not leave their computer logged on and unattended
- Change their password frequently
- Do not choose a password that's easy to guess
- Do not give their password to anyone, ever
- Back up information stored on the practice software systems regularly and store these securely and away from the practice – on line by Mark Titley
- Do not disclose any personal information without the data subject's consent or verifying the enquirer (e.g. phone the police officer or the social worker back via the station or office switch board)
- Are aware that email can be a very risky means of communicating, especially in relation to personal information
- Are careful when responding to email e.g. using 'reply all' or 'send to all' or when forwarding email
- Do not send sensitive personal information by email unless it is encrypted or anonymized
- Do not mix personal and work email accounts
- Understand that the need to maintain confidentiality forms part of their employment contracts and/or self-employed associate agreements
- Ensure that all paper waste containing any personal or confidential information is shredded securely.

## Subject Access Request

You can access to the data that we hold about you and to receive a copy by submitting a written request. There will be no charge for this.

We will provide the requested information (and an explanation if you require it) within 30 days of receiving your request.

Requests to be made in writing for the attention of your treating Dentist at;

*The Martock Dental Practice  
13 Church Street  
Martock  
TA12 6JL  
Or [reception@martockdental.co.uk](mailto:reception@martockdental.co.uk)*

## If you do not agree

If you do not wish personal data that we hold about you to be disclosed or used in the way that is described in this Code, you should discuss the matter with your dentist. You should be aware, however, that objecting to how we process your information may affect our ability to provide you with dental care.

If you feel there is an issue with the way your data is handled, you have the right to complain to the Information Commissioners Office (ICO). Their contact details are;

*Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF  
Tel: 0303 123 1113*

You can also complain online at [www.ico.org.uk/concerns/](http://www.ico.org.uk/concerns/)

<b>Produced by</b>	Emma Nash
<b>Date Created</b>	21 <sup>st</sup> May 2018
<b>Review Date</b>	May 2019
<b>Location</b>	Information Governance Policies