# DATA PROTECTION POLICY

## 1. POLICY STATEMENT

1.1 Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information about our staff, and we recognise the need to treat it in an appropriate and lawful manner. The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, customers and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations. The Act imposes restrictions on how we may use that information.

1.2 This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action.

## 2. STATUS OF THE POLICY

2.1 This policy has been approved by the Company. It sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

2.2 The Data Protection Officer is responsible for ensuring compliance with the Act and with this policy. That post is held by Paul Lambden, Head of Liaison and Risk Management. Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Protection Officer by email at paul.lambden@colosseumdental.co.uk or by phone on 07831640819.

2.3 If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with your Line Manager or the Data Protection Officer.

## 3. DEFINITION OF DATA PROTECTION TERMS

3.1 “Data” is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 “Data subjects” for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.3 “Personal data” means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data

can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

3.4 "Data controllers" are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in our business.

3.5 "Data users" include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

3.6 "Data processors" include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

3.7 "Processing" is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 "Sensitive personal data" includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

## 4. DATA PROTECTION PRINCIPLES

4.1 Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

4.1.1 Processed fairly and lawfully.
4.1.2 Processed for limited purposes and in an appropriate way.
4.1.3 Adequate, relevant and not excessive for the purpose.
4.1.4 Accurate.
4.1.5 Not kept longer than necessary for the purpose.
4.1.6 Processed in line with data subjects' rights.
4.1.7 Secure.
4.1.8 Not transferred to people or organisations situated in countries without adequate protection.

## 5. FAIR AND LAWFUL PROCESSING

5.1 The Act is intended not to prevent the processing of personal data, but to ensure

that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case it is the Company), who the data controller's representative is (in this case the Data Protection Compliance Manager), the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred. For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

## 6. PROCESSING FOR LIMITED PURPOSES

6.1 Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

## 7. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

7.1 Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

## 8. ACCURATE DATA

8.1 Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

## 9. TIMELY PROCESSING

9.1 Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required. For guidance on how long certain data is likely to be kept before being destroyed, contact the Data Protection Officer.

## 10. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

10.1 Data must be processed in line with data subjects' rights. Data subjects have a right to:

10.1.1 Request access to any data held about them by a data controller.
10.1.2 Prevent the processing of their data for direct-marketing purposes.
10.1.3 Ask to have inaccurate data amended.
10.1.4 Prevent processing that is likely to cause damage or distress to themselves or anyone else.

## 11. DATA SECURITY

11.1 We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

11.2 The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

11.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

11.3.1 “Confidentiality” means that only people who are authorised to use the data can access it.
11.3.2 “Integrity” means that personal data should be accurate and suitable for the purpose for which it is processed.
11.3.3 “Availability” means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

11.4 Security procedures include:

11.4.1 “Entry controls”. Any stranger seen in entry-controlled areas should be reported.
11.4.2 “Secure lockable desks and cupboards.” Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

11.4.3 “Methods of disposal”. Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.

11.4.4 “Equipment.” Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

## 12. DEALING WITH SUBJECT ACCESS REQUESTS

12.1 A formal request from a data subject for information that we hold about them must be made in writing. A fee is payable by the data subject for provision of this information. Any member of staff who receives a written request should forward it to the HR department immediately, who will liaise with the Data Protection Officer.

## 13. PROVIDING INFORMATION OVER THE TELEPHONE

13.1 Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

13.1.1 Check the caller's identity to make sure that information is only given to a person who is entitled to it.
13.1.2 Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.
13.1.3 Refer to their Line Manager or the Data Protection Officer for assistance in difficult situations. No-one should be bullied into disclosing personal information.

## 14. MONITORING AND REVIEW OF THE POLICY

14.1 This policy is reviewed annually by the Company.

14.2 We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.