PRACTICE DATA PROTECTION POLICY

This Dental Practice is committed to ensuring the security of personal data held by the practice. This objective is achieved by every member of the practice team complying with this policy. The practice is further committed to complying with the Data Protection Act 1998 and the GDC Standards by collecting, holding, maintaining and accessing data in an open and fair fashion.

All data is:

- processed fairly and lawfully
- obtained only for specified and lawful purposes and further processed only in a compatible manner
- adequate, relevant and not excessive to the purpose of processing
- accurate and kept up-to-date
- kept no longer than necessary
- processed in accordance with the rights of the data subjects
- kept secure and confidential
- not transferred outside the EEA unless adequate protection is provided

The practice will only keep relevant information about employees for the purposes of employment, or about patients to provide them with safe and appropriate dental care. The practice will not process any relevant 'sensitive personal data' without prior informed consent. As defined by the Act 'sensitive personal data' is that related to political opinion, racial or ethnic origin, membership of a trade union, the sexual life of the individual, physical or mental health or condition, religious or other beliefs of a similar nature. Sickness and accidents records will also be kept confidential.

Hard copy and computerised records are stored, reviewed and updated securely and confidentially. Records are securely destroyed when no longer required. Confidential information is only seen by personnel who need to see it and the team are trained on our policies and procedures to keep patient information confidential. Personnel records will only be seen by appropriate management.

Criminal record check information is kept securely in a lockable, non-portable storage cabinet with access strictly controlled and limited to persons who need to have access to this information in the course of their duties. Criminal record disclosure details (CRB/DBS checks) are not kept for longer than necessary. They are kept for no longer than six months after the decision has been made to appoint or not, from appointment or for six months from the date the applicant was unsuccessful, to allow for the consideration and resolution of any disputes or complaints.

Patients' records will only be seen by appropriate team members. To facilitate patients' health care the personal information about them may be disclosed to a doctor, health care professional, hospital, NHS authorities, the Inland Revenue, the Benefits Agency (when claiming exemption or remission from NHS charges) or private dental schemes of which the patient is a member. In all cases the information shared will be only that which is relevant to the situation. In very limited cases, such as for identification purposes, or if required by law, information may have to be shared with a party not involved in the patient's health care. In all other cases, information will not be disclosed to such a third party without the patient's written authority.

All confidential information is sent via secure methods. Electronic communications and stored data are encrypted. All computerised clinical records are backed up and encrypted copies are kept off-site.

Confidentiality (see also the practice confidentiality policy)

- All staff employment contracts contain a confidentiality clause.
- Access to personal data is on a "need to know" basis only. Access to information is monitored and breaches of security will be dealt with swiftly by Melanie Bell or Lynn Sloss
- We have procedures in place to ensure that personal data is regularly reviewed, updated and deleted in a confidential manner when no longer required. The practice adheres to the minimum legal requirements for keeping all clinical records. These are eleven years for adults and up to the age of 25 or eleven years whichever is the longer for children, although medico-legal organisations prefer that all health records are kept indefinitely. Patients and staff have the right to access their records and receive a copy, after making a request in writing and paying a fee, within 40 days of the request.
- All patients and staff members should be informed that the practice will process their personal data and if required they should be given an explanation of how the data is going to be processed and provided with a copy of the Data Protection Policy.

Physical security measures

- Personal data is only taken away from practice premises in exceptional circumstances and when authorised by Melanie Bell or Lynn Sloss. If personal data is taken from the premises it must never be left unattended in a car or in a public place.
- Personnel records are kept in a lockable fireproof cabinet, which is not easily accessible by patients and visitors to the practice.
- Efforts have been made to secure the practice against theft by, for example, the use of intruder alarms, lockable windows and doors.
- The practice has in place a business continuity plan in case of a disaster. This includes procedures set out for protecting and restoring personal data.

Information held on computer

- appropriate software controls are used to protect computerised records, for example the use of passwords and encryption. Passwords are only known to those who require access to the information, are changed on a regular basis and are not written down or kept near or on the computer for others to see. All users should log off the computer when not present in the surgery /Reception/office.
- Daily and weekly back-ups of computerised data are taken and stored in the safe. Back-ups are also tested at prescribed intervals to ensure that the information being stored is usable - should it be needed
- Staff using practice computers will undertake computer training to avoid unintentional deletion or corruption of information
- Dental computer systems all have a full audit trail facility – preventing the erasure or overwriting of data. The system records details of any amendments made to data, who made them and when.

- Precautions are taken to avoid loss of data through the introduction of computer viruses Security Measures

This statement has been issued to existing staff who have access to personal data at the practice and will be given to new staff during induction. Should any staff have concerns about the security of personal data within the practice they should contact Melanie Bell or Lynn Sloss.

Access to records

Patients and team members can have access to the original of the records kept about them free of charge. To receive a copy of all records kept about them by the practice a team member or a patient should make a written request to the Practice Manager together with a payment of £10 for computerised records or £50 for a mixture of computerised and manual records and non-computerised radiographs. The Practice Manager will provide a copy within a period of 40 days. An employee or a patient may challenge information held on record and following investigation should the information be inaccurate the practice will correct the information and inform the patient or the team member of the change in writing.

This policy should be read in conjunction with Confidentiality Policy, and the Information Governance Policy.