Information Security 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.

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 [*contact name*]
- We have procedures in place to ensure that personal data is regularly reviewed, updated and deleted in a confidential manner when no longer required. For example, we keep patient records for at least 11 years or until the patient is aged 25 – whichever is the longer.

Physical security measures

- Personal data is only taken away from the practice premises in exceptional circumstances and when authorised by [*contact name*]. If personal data is taken from the premises it must never be left unattended in a car or in a public place.
- 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
- Daily and weekly back-ups of computerised data are taken and stored in a fireproof container, off-site. 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

This statement has been issued to existing staff with 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 Dr Jeremy Breckon.*

Adopted: 14 February 2011