Practice Information Security

Brookview Dental Care is committed to ensuring the security of personal data held by the practice.

Confidentiality

- All staff employment contracts contain a confidentiality clause, and all staff sign a confidentiality agreement
- 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 Niki Kitsiou.
- Procedures are in place to ensure that personal data is reviewed regularly and updated/ deleted in a confidential manner when required. For example, we keep patient records for at least 11 years or until the patient is 25 years old, whichever is longer

Physical Security Measures

- Personal data is only taken away from the practice premises in exceptional circumstances and when authorised by Niki Kitsiou. If personal data is taken from the premises it must never be left unattended in a car or 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, for example the use of intruder alarms, locked windows and doors.
- The practice has a business continuity plan in place 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, and are not written down.
- Daily backups of computerised data are stored off-site on two encrypted drives.
- A managed anti-virus program is installed on all computers in the practice.