Data Security Policy

Trinity Dental is committed to ensuring the security of personal data held by the clinic. This policy is issued to existing staff with access to personal data at the clinic and will be given to new staff during induction. Should any staff have concerns about the security of personal data within the clinic they should contact the clinic manager. All members of the team must comply with this policy.

Confidentiality

1. All employment contracts and contracts for services contain a confidentiality clause, which includes a commitment to comply with the clinic confidentiality policy.

2. 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 the clinic manager.

3. 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 10 years or until the patient is aged 25 – whichever is the longer.

Physical security measures

4. Personal data is only taken away from the clinic premises in exceptional circumstances and when authorised by the director or the business manager. If personal data is taken from the premises it must never be left unattended in a car or in a public place.

5. Records that have been printed are kept in a lockable fireproof cabinet, which is not easily accessible by patients and visitors to the clinic.

6. Efforts have been made to secure the clinic against theft by, for example, the use of intruder alarms, lockable windows and doors.

7. The clinic 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

8. Appropriate software controls are used to protect computerised records, for example the use of passwords, pseudonymisation 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.

9. 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.

10. Staff using company computers will undertake the appropriate training to avoid unintentional deletion or corruption of information.

11. 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.

12. Precautions are taken to avoid loss of data through the introduction of computer viruses and are protected and supported by a reputable IT support company.

Policy Date: September 2019
Review Date: September 2020
Initials: RS