Data security policy

This dental practice is committed to ensuring the security of personal data held by the practice and complying with GDPR General Data Protection Regulations. This policy is issued to all staff with access to personal data at the practice and will be given to new staff during their induction. If any member of the team has concerns about the security of personal data within the practice, they should contact Benjamin Lauffer.

All members of the team must comply with this policy.

Confidentiality

- All employment contracts and contracts for services contain a confidentiality clause, which includes a commitment to comply with the practice confidentiality policy
- 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 Benjamin Lauffer.
- We have procedures in place to ensure that personal data is regularly reviewed, updated and, when no longer required, deleted in a confidential manner. For example, we keep patient records for at least 10 years or until the patient is aged 25 – whichever is the longer.
- We use data protection by design to aim to ensure that only the minimum necessary personal data is processed, that pseudonymisation is used where possible, that processing is transparent, where feasible allowing individuals to monitor what is being done with their data.

Physical security measures

- Personal data is only removed from the practice premises in exceptional circumstances and when authorised by Benjamin Lauffer. 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 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 undertake computer training to avoid unintentional deletion or corruption of information
- Dental computer systems 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.

Loss of patient information

- Any loss, damage to or unauthorised disclosure of patient information must be reported immediately to Benjamin Lauffer immediately.

Date	12/10/2023
Review Date	Oct 2024
By	KS