Data Security Policy

The practice is committed to ensuring that the security of personal data held by the practice. This policy is issued to all staff with access to personal data at the practice and is given to new staff during induction. If any member of the team has concerns about the security of personal data within the practice they should discuss these with Dr Khan.

As Data Protection Officer, Dr Sadaf Khan has ultimate responsibility for Data Security within the Practice, with the Practice Manager as his deputy.

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 Dr Sadaf Khan
- 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.

Physical security measures

- Personal data is only removed from the practice premises in exceptional circumstances and when authorised by Dr Sadaf Khan. 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 back-ups of computerised data are taken and stored 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 are competent in their use. This helps avoid unintentional deletion or corruption of information
- The patient data system has 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

Information held on computer

- Any loss, damage to or unauthorised disclosure of patient information must be reported immediately to Dr Sadaf Khan

Name	**Dr Sadaf Khan**
Date	**September 2017 (updated May 2018)**
Review date	**August 2018**