Data Security Policy

Hurst Dental Practice is committed to ensuring the security of personal data help 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 Mrs Anu Jawahar.
- 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 patients records for at least 11 years or until the patient is 25 – whichever is the longer.

Physical security measures

- Personal date is only taken away from the practice premises in exceptional circumstances and when authorised by Mrs. Anu Jawahar.
- If personal data is taken from the premises it must never be left unattended in a car or in a public place.
- Paper records are kept in a part of the practice which is physically separated from public areas and is not eastly 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 if a disaster. This includes procedures set out for protecting and restoring personal date.

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 f computerised data are taken and stored off-site. Back-ups are also tested occasionally to ensure that the information being stored is usable should it be needed.

- Dental computer systems all have a full audit trail facility preventing the erasure or overwriting of date. The system records details of any amendments make to the date, who made them and when.
- Precautions are taken to avoid loss of date through the introduction of computer viruses.

This statement had been issued to existing staff with access to personal date at the practice and will be given to new staff during their induction. Should any staff have concerns about the security of personal data within the practice they should contact Mrs. Anu Jawahar.